BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号

特開平11－88859

(43)公開日　平成11年(1999)３月30日

(51)Int.Cl.[6]	識別記号	ＦＩ	
Ｈ０４Ｎ　7/167		Ｈ０４Ｎ　7/167	Ｚ
Ｇ０６Ｆ　12/14	３２０	Ｇ０６Ｆ　12/14	３２０Ｂ
			３２０Ｅ
Ｇ０９Ｃ　1/00	６６０	Ｇ０９Ｃ　1/00	６６０Ｄ
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１

審査請求　有　請求項の数41　ＯＬ　外国語出願　（全 60 頁）

(21)出願番号　特願平10－155092

(22)出願日　平成10年(1998)６月４日

(31)優先権主張番号　０８／８８１１３９

(32)優先日　1997年６月24日

(33)優先権主張国　米国（ＵＳ）

(71)出願人　390009531
インターナショナル・ビジネス・マシーンズ・コーポレイション
INTERNATIONAL BUSINESS MASCHINES CORPORATION
アメリカ合衆国10504、ニューヨーク州アーモンク　（番地なし）

(72)発明者　マーク・ルイス・シアセリ
アメリカ合衆国13760、ニューヨーク州エンディコット、パイン・ノール・ロード、140

(74)代理人　弁理士　坂口　博　（外１名）

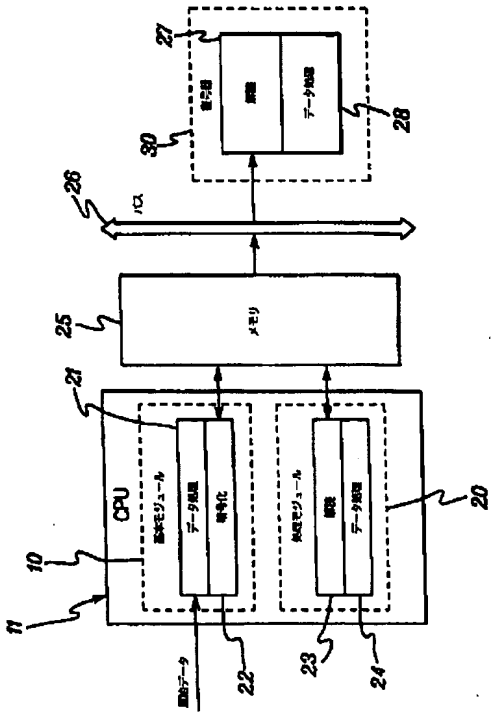
最終頁に続く

(54)【発明の名称】　コンピュータ・システムにおけるコピーライト・データの保護方法及び装置

(57)【要約】

【課題】　暗号化された符号化データ・ストリームの従来のＤＶＤ処理を改善することである。

【解決手段】　例えばＣＳＳ技術に従い暗号化されたデータ・ストリームを、デジタル的に処理する装置、方法、及びコンピュータ・プログラム製品が提供される。このデジタル処理は、中央処理ユニット（ＣＰＵ）から、メモリやシステム・バスなどの任意のアクセス可能な構造への、コンピュータ・システム内における生データの通信に保険をかける。ＣＳＳ暗号化データ・ストリームの解読は、ＣＰＵ上で実行されるモジュール内で発生し、次にＣＰＵからの転送に先立ち、データの再暗号化が実行される。データをこのように処理することにより、ＣＳＳ暗号化データ・ストリームのソフトウェア解読を可能にする一方で、著作権を有する資料の保全性が保持される。使用される暗号化／解読アルゴリズム対を確立する様々な技術が、述べられる。



【特許請求の範囲】

【請求項１】暗号化データ・ストリームを受信するように接続される中央処理ユニット（ＣＰＵ）を有するコンピュータ・システム内で、前記暗号化データ・ストリームを処理する装置であって、

受信された前記暗号化データ・ストリームを解読し、生のデータ・ストリームを生成する前記ＣＰＵ内の第１の解読手段と、

前記暗号化データ・ストリームとは異なる暗号化アルゴリズムにより、前記生のデータ・ストリームを再暗号化し、暗号化データ・ストリームを生成する前記ＣＰＵ内の再暗号化手段と、

前記暗号化データ・ストリームを前記ＣＰＵから、該ＣＰＵに接続される前記コンピュータ・システムの第２の構造に転送する手段と、

前記第２の構造から前記暗号化データ・ストリームを受信し、該暗号化データ・ストリームを解読し、前記生のデータ・ストリームを生成する、前記第２の構造に接続される第２の解読手段とを含み、前記ＣＰＵ内の前記第１の解読手段が、受信された前記暗号化データ・ストリームの解読を実行する一方で、前記生のデータ・ストリームが、前記ＣＰＵから、該ＣＰＵに接続される前記第２の構造に転送される際に暴露されないようにする、装置。

【請求項２】前記暗号化データ・ストリームが、暗号化された符号化データ・ストリームを含み、前記装置が、前記第２の解読手段により生成される生の符号化データ・ストリームを復号する、前記第２の解読手段に接続される復号器を含む、請求項１記載の装置。

【請求項３】前記生の符号化データ・ストリームがビデオ・データ・ストリームを含み、前記復号器がＭＰＥＧビデオ復号器を含む、請求項２記載の装置。

【請求項４】前記暗号化された符号化データ・ストリームが、ＣＳＳ暗号化されたＭＰＥＧ符号化データ・ストリームを含み、前記第１の解読手段が、前記暗号化された符号化データ・ストリームを前記ＣＰＵ内でＣＳＳ解読する手段を含み、前記復号器が前記生の符号化データ・ストリームをＭＰＥＧ復号する手段を含む、請求項２記載の装置。

【請求項５】前記復号器が復号ハードウェア装置を含み、前記第２の解読手段が前記復号ハードウェア装置内に存在する、請求項２記載の装置。

【請求項６】前記再暗号化手段が、前記生のデータ・ストリームを再暗号化するために使用されるキーを提供する手段を含み、前記第２の解読手段が前記キーを用いて、前記暗号化データ・ストリームを解読する手段を含む、請求項１記載の装置。

【請求項７】前記再暗号化手段が、前記キーを暗号化して暗号化キーを生成し、前記暗号化キー及び前記暗号化データ・ストリームを、前記ＣＰＵに接続される前記第２の構造への転送のために、多重化データ・ストリームに多重化する手段を含み、前記第２の解読手段が、前記多重化データ・ストリームを多重化解除し、前記暗号化キー及び前記暗号化データ・ストリームを獲得する手段と、前記暗号化キーを解読する手段とを含む、請求項６記載の装置。

【請求項８】前記再暗号化手段及び前記第２の解読手段により使用される暗号化／解読アルゴリズム対を選択する手段を含む、請求項１記載の装置。

【請求項９】前記選択手段が、選択された前記暗号化／解読アルゴリズム対の解読アルゴリズムを、前記再暗号化手段から前記第２の解読手段にダウンロードする手段を含み、前記ダウンロードする手段が、前記再暗号化手段と前記第２の解読手段との間の転送のために、前記解読アルゴリズムを暗号化する手段を含む、請求項８記載の装置。

【請求項１０】前記選択手段が、前記再暗号化手段及び前記第２の解読手段において、複数の暗号化／解読アルゴリズム対から、前記暗号化／解読アルゴリズム対を選択する手段を含み、前記選択手段が前記第２の解読手段に、前記複数の暗号化／解読アルゴリズム対の内で、前記再暗号化手段により使用される暗号化アルゴリズムに対応する解読アルゴリズムを知らせる手段を含む、請求項８記載の装置。

【請求項１１】前記第２の解読手段が前記ＣＰＵ内に配置される解読モジュールを含み、前記ＣＰＵに接続される前記第２の構造がメモリを含む、請求項１記載の装置。

【請求項１２】データ・ストリームを受信するように接続される中央処理ユニット（ＣＰＵ）を有するコンピュータ・システム内で、前記データ・ストリームを処理する装置であって、

前記データ・ストリーム内で識別される著作権データを暗号化し、暗号化データを生成する、前記ＣＰＵ内の暗号化手段と、

前記著作権データだけを前記暗号化データとして、前記ＣＰＵから、該ＣＰＵに接続される前記コンピュータ・システムの構造に転送する手段と、

前記暗号化データを受信する前記構造に接続され、前記暗号化データを解読する手段を含む解読手段と、

を含む、装置。

【請求項１３】前記ＣＰＵ内で、前記データ・ストリームの前記著作権データを識別する手段を含み、該識別手段が識別された前記著作権データを前記暗号化手段に提供する、請求項１２記載の装置。

【請求項１４】前記データ・ストリームが暗号化された符号化データ・ストリームを含み、前記装置が、前記暗号化された符号化データ・ストリームを前記ＣＰＵ内で解読し、生の符号化データ・ストリームを生成する解読手段を含み、前記識別手段が前記生の符号化データ・ス

トリームを調査し、前記暗号化手段による暗号化のために著作権データを識別する、請求項１３記載の装置。

【請求項１５】前記解読手段がマイクロコード解読装置を含む、請求項１２記載の装置。

【請求項１６】前記データ・ストリームが暗号化データ・ストリームを含み、前記装置が、前記暗号化手段による、識別された前記著作権データの前記暗号化に先立ち、前記暗号化データ・ストリームを解読する手段を含み、前記暗号化データ・ストリームが、前記暗号化手段により生成される前記暗号化データとは異なる暗号化アルゴリズムから生成される、請求項１２記載の装置。

【請求項１７】前記暗号化手段が、識別された前記著作権データの前記暗号化において、及び前記解読手段による、前記暗号化データの解読のために使用されるキーを提供する手段を含む、請求項１２記載の装置。

【請求項１８】前記暗号化手段が前記キーを暗号化して暗号化キーを生成し、前記暗号化キー及び前記暗号化データを、前記ＣＰＵに接続される前記構造への転送のために、多重化データ・ストリームに多重化する手段を含み、前記解読手段が、前記多重化データ・ストリームを多重化解除し、前記暗号化キー及び前記暗号化データを獲得する手段と、前記暗号化キーを解読する手段とを含む、請求項１７記載の装置。

【請求項１９】複数の予め定義された暗号化／解読アルゴリズム対から、前記再暗号化手段及び前記解読手段により使用される暗号化／解読アルゴリズム対を選択する手段を含み、選択された前記暗号化／解読アルゴリズム対が、前記暗号化手段により使用される暗号化アルゴリズムと、前記解読手段により使用される対応する解読アルゴリズムとを含む、請求項１２記載の装置。

【請求項２０】中央処理ユニット（ＣＰＵ）及び該ＣＰＵに接続される構造を有するコンピュータ・システム内で、暗号化データ・ストリームを処理する方法であって、

ａ）前記ＣＰＵにおいて、前記暗号化データ・ストリームを受信するステップと、

ｂ）前記ＣＰＵ上で実行されるモジュール内で、前記暗号化データ・ストリームを解読し、生のデータを生成するステップと、

ｃ）前記生のデータを前記ＣＰＵ内で再暗号化し、少なくとも部分的に暗号化されたデータを生成するステップと、

ｄ）前記再暗号化に続き、前記少なくとも部分的に暗号化されたデータを、前記ＣＰＵから、該ＣＰＵに接続される前記コンピュータ・システムの第２の構造に転送するステップと、

ｅ）前記転送に続き、前記少なくとも部分的に暗号化されたデータを検索して解読し、生のデータを生成するステップと、

を含み、前記解読が前記ＣＰＵ上で実行される前記モジュール内で発生する一方で、前記生のデータが前記ＣＰＵから、該ＣＰＵに接続される前記構造に転送される際に、暴露されないようにし、前記暗号化データ・ストリームが、前記少なくとも部分的に暗号化されたデータを生成する前記再暗号化ステップｃ）により使用されるのとは異なる暗号化アルゴリズムから生成される、方法。

【請求項２１】前記暗号化データ・ストリームが暗号化された符号化データ・ストリームを含み、前記解読ステップｅ）が生の符号化データを生成するステップを含み、前記方法が、前記生の符号化データを復号し、前記生のデータを生成するステップを含む、請求項２０記載の方法。

【請求項２２】前記暗号化された符号化データ・ストリームが、ＣＳＳ暗号化されたＭＰＥＧ符号化データ・ストリームを含み、前記解読ステップｂ）が、前記暗号化された符号化データ・ストリームを前記ＣＰＵ内でＣＳＳ解読するステップを含み、前記復号ステップが、前記生の符号化データをＭＰＥＧ復号し、前記生のデータを生成するステップを含む、請求項２１記載の方法。

【請求項２３】前記再暗号化ステップｃ）が、キーを用いて前記生のデータを暗号化するステップを含み、前記方法が、前記解読ステップｅ）のために前記キーを提供するステップを含み、前記解読ステップが前記キーを用いて、前記少なくとも部分的に暗号化されたデータを解読する、請求項２０記載の方法。

【請求項２４】前記再暗号化ステップｃ）が、前記キーを暗号化して暗号化キーを生成し、前記暗号化キー及び前記少なくとも部分的に暗号化されたデータを多重化データ・ストリームに多重化するステップを含み、前記解読ステップｅ）が、前記多重化データ・ストリームを多重化解除し、前記暗号化キー及び前記少なくとも部分的に暗号化されたデータを獲得するステップと、前記暗号化キーを解読し、前記キーを用いて、前記少なくとも部分的に暗号化されたデータを解読するステップとを含む、請求項２３記載の方法。

【請求項２５】複数の予め定義された暗号化／解読アルゴリズム対から、前記再暗号化ステップｃ）及び前記解読ステップｅ）により使用される暗号化／解読アルゴリズム対を選択するステップを含む、請求項２０記載の方法。

【請求項２６】前記再暗号化ステップｃ）が前記選択ステップを実行し、前記再暗号化ステップが、前記解読ステップｅ）により使用される前記暗号化／解読アルゴリズム対の解読アルゴリズムをダウンロードするステップを含む、請求項２５記載の方法。

【請求項２７】前記解読ステップｅ）が、前記少なくとも部分的に暗号化されたデータを前記ＣＰＵ内で解読するステップを含み、前記ＣＰＵに接続される前記構造がメモリ構造を含み、前記検索ステップｅ）が、前記メモリ構造から、前記少なくとも部分的に暗号化されたデー

タを検索するステップを含む、請求項２０記載の方法。
【請求項２８】中央処理ユニット（ＣＰＵ）と、該ＣＰＵの外部にあって該ＣＰＵに接続される構造とを有するコンピュータ・システム内で、データ・ストリームを処理する方法であって、
ａ）前記ＣＰＵにおいて、前記データ・ストリームを受信するステップと、
ｂ）前記データ・ストリーム内で識別される著作権データを暗号化し、暗号化データを生成するステップと、
ｃ）前記暗号化ステップｂ）に続き、前記著作権データだけを前記暗号化データとして、前記ＣＰＵから該ＣＰＵに接続される構造に転送するステップと、
ｄ）前記ＣＰＵに接続される前記構造から前記暗号化データを検索し、該暗号化データを解読して、生のデータを生成するステップと、
を含み、前記解読ステップが、前記暗号化データを前記ＣＰＵの外部の前記構造へ転送した後に発生し、前記生のデータが、前記ＣＰＵと該ＣＰＵに接続される前記構造との間で転送される際に、前記コンピュータ・システム内で暴露されないようにする、方法。
【請求項２９】前記暗号化ステップｂ）により使用される前記データ・ストリームの前記著作権データを、前記ＣＰＵ内で識別するステップを含む、請求項２８記載の方法。
【請求項３０】前記データ・ストリームが暗号化データ・ストリームを含み、前記方法が、前記著作権データの前記識別に先立ち、前記暗号化データ・ストリームを解読するステップを含み、前記暗号化データ・ストリームが、前記暗号化ステップｂ）により使用されるのとは異なる暗号化アルゴリズムから生成される、請求項２９記載の方法。
【請求項３１】前記暗号化ステップｂ）が、識別された前記著作権データをキーを用いて暗号化し、前記キーを前記解読ステップｄ）に提供するステップを含む、請求項２８記載の方法。
【請求項３２】前記暗号化ステップｂ）が前記キーを暗号化して暗号化キーを生成し、前記暗号化キー及び前記暗号化データを、前記ＣＰＵに接続される前記構造への転送のために、多重化データ・ストリームに多重化するステップを含み、前記解読ステップｄ）が、前記多重化データ・ストリームを多重化解除し、前記暗号化キー及び前記暗号化データを獲得するステップと、前記暗号化データの解読のために使用する前記暗号化キーを解読するステップとを含む、請求項３１記載の方法。
【請求項３３】複数の予め定義された暗号化／解読アルゴリズム対から、暗号化／解読アルゴリズム対を選択するステップを含み、前記暗号化ステップｂ）が、選択された前記暗号化／解読アルゴリズム対の暗号化アルゴリズムを用いて、識別された前記著作権データを暗号化し、前記解読ステップｄ）が、選択された前記暗号化／解読アルゴリズム対の対応する解読アルゴリズムを用い、前記暗号化データを解読するステップを含む、請求項２８記載の方法。
【請求項３４】中央処理ユニット（ＣＰＵ）及び該ユニットに接続される構造を有するコンピュータ・システム内で、暗号化データ・ストリームを処理するために使用されるコンピュータ読出し可能プログラム・コード手段を有するコンピュータ使用可能媒体を含むコンピュータ・プログラム製品であって、前記ＣＰＵにおいて前記暗号化データ・ストリームを受信し、前記ＣＰＵ内で前記暗号化データ・ストリームを解読し、生のデータを生成し、該生のデータを前記ＣＰＵ内で再暗号化し、少なくとも部分的に暗号化されたデータを生成する、コンピュータ読出し可能プログラム・コード手段と、前記少なくとも部分的に暗号化されたデータを、前記ＣＰＵから該ＣＰＵに接続される前記構造に転送する、コンピュータ読出し可能プログラム・コード手段と、前記ＣＰＵに接続される前記構造から、前記少なくとも部分的に暗号化されたデータを検索し、前記少なくとも部分的に暗号化されたデータを解読して、生のデータを生成する、コンピュータ読出し可能プログラム・コード手段とを含み、前記解読が前記ＣＰＵ内で発生する一方で、前記生のデータが、前記ＣＰＵから該ＣＰＵに接続される前記構造に転送される際に、暴露されないようにする、コンピュータ・プログラム製品。
【請求項３５】前記暗号化データ・ストリームが、暗号化された符号化データ・ストリームを含み、前記コンピュータ・プログラム製品が、前記少なくとも部分的に暗号化されたデータを解読する前記コンピュータ読出し可能プログラム・コード手段により生成された生の符号化データを復号する、コンピュータ読出し可能プログラム・コード手段を含む、請求項３４記載のコンピュータ・プログラム製品。
【請求項３６】前記暗号化された符号化データ・ストリームが、ＣＳＳ暗号化されたＭＰＥＧ符号化データ・ストリームを含み、前記暗号化された符号化データ・ストリームを解読する前記コンピュータ読出し可能コード手段が、前記暗号化された符号化データ・ストリームをＣＳＳ解読するコンピュータ読出し可能プログラム・コード手段を含み、前記復号のためのコンピュータ読出し可能プログラム・コード手段が、前記生の符号化データ・ストリームをＭＰＥＧ復号するコンピュータ読出し可能プログラム・コード手段を含む、請求項３５記載のコンピュータ・プログラム製品。
【請求項３７】中央処理ユニット（ＣＰＵ）と、該ＣＰＵの外部にあって該ＣＰＵに接続される構造とを有するコンピュータ・システム内で、データ・ストリームを処理するために使用されるコンピュータ読出し可能プログラム・コード手段を有するコンピュータ使用可能媒体を含むコンピュータ・プログラム製品であって、

前記ＣＰＵにおいて前記データ・ストリームを受信し、該データ・ストリーム内で識別される著作権データを暗号化し、暗号化データを生成する、コンピュータ読出し可能プログラム・コード手段と、
前記暗号化データを、前記ＣＰＵから該ＣＰＵの外部の前記構造に転送する、コンピュータ読出し可能プログラム・コード手段と、
前記ＣＰＵの外部の前記構造への転送の後、前記暗号化データを検索して解読する、コンピュータ読出し可能プログラム・コード手段と、
を含み、前記生のデータが、前記ＣＰＵと該ＣＰＵに接続される前記構造との間の転送に際し、前記コンピュータ・システム内で暴露されないようにする、コンピュータ・プログラム製品。
【請求項３８】前記データ・ストリームの前記著作権データを識別して暗号化する、コンピュータ読出し可能プログラム・コード手段を含む、請求項３７記載のコンピュータ・プログラム製品。
【請求項３９】識別された前記著作権データを暗号化する前記コンピュータ読出し可能プログラム・コード手段が、キーを用いて前記暗号化を実行し、前記キーを前記暗号化データを解読する前記コンピュータ読出し可能プログラム・コード手段に提供する、コンピュータ読出し可能プログラム・コード手段を含む、請求項３７記載のコンピュータ・プログラム製品。
【請求項４０】前記暗号化のためのコンピュータ読出し可能プログラム・コード手段が、前記キーを暗号化して、暗号化キーを生成し、前記暗号化キー及び前記暗号化データを、前記ＣＰＵに接続される前記構造への転送のために、多重化データ・ストリームに多重化するコンピュータ読出し可能プログラム・コード手段を含み、前記解読のためのコンピュータ読出し可能プログラム・コード手段が、前記多重化データ・ストリームを多重化解除し、前記暗号化キー及び前記暗号化データを獲得し、前記暗号化データの解読のために使用する前記暗号化キーを解読するコンピュータ読出し可能プログラム・コード手段を含む、請求項３９記載のコンピュータ・プログラム製品。
【請求項４１】識別された前記著作権データの暗号化、及び前記暗号化データの解読において使用される暗号化／解読アルゴリズム対を、複数の予め定義された暗号化／解読アルゴリズム対から選択するコンピュータ読出し可能プログラム・コード手段を含み、前記暗号化データを解読する前記コンピュータ読出し可能プログラム・コード手段に、選択された前記暗号化／解読アルゴリズム対の対応する解読アルゴリズムを知らせる、コンピュータ読出し可能プログラム・コード手段を含む、請求項３７記載のコンピュータ・プログラム製品。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は一般に、デジタル・ビデオ／音声データを保護する装置及び方法に関し、特に、非暗号化形式のデータをメモリまたはバスなどのアクセス可能な構造において暴露することなく、ＣＰＵからこれらの内部構造へ通信するための、コンピュータ・システム内でのデータの暗号化／解読のための装置、方法及びコンピュータ・プログラム製品に関する。
【０００２】
【従来の技術】過去１０年間に、世界的な電子通信システムにより、人々が情報を送受信する方法が向上した。特に、リアルタイム・ビデオ及び音声システムの能力は、ここ数年の間に著しく改善した。ビデオ・オン・デマンド、ビデオ会議及びデジタル・ビデオ・ディスク（ＤＶＤ）映画などのサービスを提供するためには、巨大な量の帯域幅が要求される。実際に帯域幅は、しばしばこうしたシステムの有効性の第１の阻害要因となる。
【０００３】既存の技術により課せられる制約を克服するために、圧縮システムが登場した。これらのシステムは、ピクチャ・シーケンス内の冗長性を除去することにより、伝送されなければならないビデオ及び音声データの量を低減する。受信端末において、ピクチャ・シーケンスが圧縮解除され、リアルタイムに表示され得る。
【０００４】登場したビデオ圧縮規格の１つの例は、ＭＰＥＧ（Moving Picture Experts Group）規格である。ＭＰＥＧ規格では、ビデオ圧縮がピクチャ内及びピクチャ間の両方において定義される。ピクチャ内のビデオ圧縮は、離散コサイン変換、量子化、可変長符号化、及びハフマン符号化による、時間ドメインから周波数ドメインへのデジタル・イメージの変換により達成される。ピクチャ間のビデオ圧縮は、"動き予測"と呼ばれるプロセスを介して達成され、そこでは動きベクトルと差分データとの和が、あるピクチャから別のピクチャへの画素のセットの変換を記述するために使用される。ＩＳＯ ＭＰＥＧ２規格は、ビットストリームの構文及び復号プロセスのセマンティックス（意味）だけを指定する。符号化パラメータの特定の選択、及び性能対複雑度のトレードオフは、システム開発者に委ねられる。
【０００５】デジタル・バーサタイル・ディスク（ＤＶＤ）は、現在登場しつつある技術であり、これはその性質により、動きピクチャなどのデータを無許可の複写から保護するために、拡張的な暗号化を要求する。
【０００６】ＤＶＤはビデオ、音声並びに、ＤＶＤ復号器により、再生ビデオ、音声及び例えばサブタイトル・データとして使用される他の圧縮データの内容に対する仕様である。ＤＶＤビデオ・データは、ＭＰＥＧ規格（ＩＳＯ／ＩＥＣ１３８１８－２）により指定される。この規格により表現される他に、データはまた業界のＣＳＳ（Content Scrambling System）を用いて暗号化され、それによりＤＶＤ再生のための暗号化された符号化データ・ストリームが生成される。このデータ・ストリ

ームは、ＣＳＳ解読を実行するために認可されたハードウェアにより解読され得る。従来、ＣＳＳ解読はＰＣＩカードにおいて実行され、ＰＣＩカードは更に、暗号化された符号化データ信号のＭＰＥＧ伸長も含む。

【０００７】

【発明が解決しようとする課題】本発明の目的は、特定の１態様において、暗号化された符号化データ・ストリームのこの従来のＤＶＤ処理を改善することである。

【０００８】

【課題を解決するための手段】要するに、本発明は第１の態様において、暗号化データ・ストリームを受信するように接続された中央処理ユニット（ＣＰＵ）を有するコンピュータ・システム内で、暗号化データ・ストリームを処理する装置を含む。該装置は、受信された暗号化データ・ストリームを解読し、それにより生のデータ・ストリームを生成する解読手段を中央処理ユニット内に含む。同様に、中央処理ユニット内の再暗号化手段が生のデータ・ストリームを再暗号化し、暗号化データ・ストリームを生成する。その点で、受信される暗号化データ・ストリームは、再暗号化データ・ストリームとは異なる暗号化アルゴリズムから生成される。再暗号化データ・ストリームを中央処理ユニットから、該ユニットに接続されるコンピュータ・システムの第２の構造に転送する手段が提供される。第２の構造に接続される解読手段が、再暗号化データ・ストリームを受信して解読し、生のデータ・ストリームを生成する。生のデータ・ストリームは、中央処理ユニットから該ユニットに接続される第２の構造に転送されるときに暴露されず、一方、中央処理ユニット内の解読手段が、受信された暗号化データ・ストリームをソフトウェアにより解読する。

【０００９】別の態様では、データ・ストリームを受信するように接続される中央処理ユニットを有するコンピュータ・システム内で、該データ・ストリームを処理する装置が提供される。該装置はデータ・ストリーム内の識別された著作権データを暗号化し、そこから暗号化データを生成する暗号化手段を、中央処理ユニット内に含む。更に暗号化データを中央処理ユニットから、該ユニットに接続されるコンピュータ・システムの構造に転送する手段が提供され、著作権データだけが中央処理ユニットから、前記暗号化データとして転送される。解読手段が暗号化データを受信する構造に接続され、暗号化データを解読する。

【００１０】上で要約された態様の各々に対する様々な向上が述べられ、特許請求される。更に、対応する方法及びコンピュータ・プログラム製品が提供され、同様に特許請求される。

【００１１】再度述べるが、本発明によれば、生のデータは圧縮されるか否かに関わらず、該データの盗難を防止するために、ホスト・メモリ・バッファやシステム・バスなどの、アクセス可能なコンピュータ・システム構造内に存在することが許可されない。本発明は特に、デジタル・ビデオ・ディスク（ＤＶＤ）技術などにより使用されるＭＰＥＧ符号化、及びＣＳＳ暗号化ビデオ・データに適用可能である。ここで提供される解読技術は、例えば暗号化／解読アルゴリズム対の新たなマイクロコードをダウンロードする柔軟性を通じて続く変化を可能にする。更に、使用される特定の暗号化／解読アルゴリズムが変化し得る。概念的には、ホスト・ソフトウェアにより解読プロセスを開始し、中央処理ユニットにおいて、異なる暗号化技術を用いてデータを再暗号化し、受信モジュールにおいて、データの解読を完了する。その際、受信モジュールは、中央処理ユニット上で実行される追加のソフトウェア・モジュールを含んでもよいし、或いは中央処理ユニットに接続されるシステム・バス上に存在する復号器などの受信ハードウェア装置を含んでもよい。受信された暗号化データの基本ソフトウェア解読に続く再暗号化は、完全であるかまたは部分的である。受信モジュールにおいて、再暗号化されたデータが解読され、表示されたり音声カードを介して出力されるか、或いは他の処理を受ける。

【００１２】

【発明の実施の形態】一般的に、本発明は、例えばＣＳＳ技術を用いて暗号化されたデータ・ストリームを処理する装置、方法、及びコンピュータ・プログラム製品を含む。１態様として、本発明は中央処理ユニットにおいて、受信されたＣＳＳ暗号化信号を解読するステップを含み、続いてメモリまたはシステム・バスなどの、ＣＰＵの外部のアクセス可能な任意の構造内で、解読データの生のコピーを暴露しないようにする。このことは、ＣＳＳ暗号化ストリームのソフトウェア解読を可能にする一方で、機密保護データまたは著作権を保護された資料（ここでは集合的に"著作権データ"と呼ぶ）などの保護されるべきデータが、（データ転送の間に）原始データ・ストリームの違法な複写が容易なポイントにおいて、暴露されないことを保証する。ここで述べられる特定の例では、暗号化ストリームはまた、ＭＰＥＧ規格（ＩＳＯ／ＩＥＣ１３８１８－２）を用いて圧縮されたビデオ／音声データの符号化ストリームも含み得る。

【００１３】本発明によれば、中央処理ユニット内の基本ソフトウェア・モジュールが、ＣＳＳ解読を実行し、次に選択された暗号化／解読アルゴリズムを用いて、データ・ストリームを暗号化する。この暗号化は、任意の著作権データを例えばメモリまたはシステム・バスを通じて、ＣＰＵの外部のソフトウェア・モジュールまたはハードウェア装置の一方または両方に送信する以前に実行される。外部ソフトウェア・モジュールまたはハードウェア装置の一方または両方は、再暗号化データ・ストリームを受信すると、次にそのデータ・ストリームを解読し、それを処理する。すなわち、例えばビデオ・データの場合には、それを表示処理し、音声データの場合に

は、音声カードに出力したりする。

【００１４】要するに、ここで含まれる処理には、基本ソフトウェア・モジュールにおいて、データがコンピュータ・システムのＣＰＵからの続く伝送の間に、保護される必要があるか否かを判断するステップが含まれる。肯定の場合、基本モジュールはソフトウェア・モジュールまたはハードウェア装置の一方または両方に、究極的に、暗号化／解読アルゴリズム対を確立するためのデータのストリームを受信するように伝える。この通信は、解読アルゴリズムを受信側のソフトウェア・モジュールまたはハードウェア装置の一方または両方にダウンロードするか、或いは解読ソフトウェア／ハードウェアに、予め定義された複数の暗号化／解読アルゴリズム対の内で、実際に使用される解読アルゴリズムを伝えるステップを含み得る。基本モジュールは選択された暗号化アルゴリズムを用いて、解読されたデータを再暗号化し、データをメモリやシステム・バスなどの任意のアクセス可能な構造を通じて、最終的な解読を実行する受信側のソフトウェア・モジュールまたはハードウェア装置に転送する。受信モジュールもまた、中央処理ユニット内に配置され得るが、これはデータを解読し、通常の処理をその上で実行する。代替例として、中央処理ユニットからの再暗号化データが、システム・メモリまたはシステム・バスの一方または両方を通じて、ビデオ復号器に送信され、ビデオ復号器がデータを解読後、例えば表示のためにそれを復号する。

【００１５】図１は、本発明に従う装置を使用するコンピュータ・システムの１実施例を示す。基本ソフトウェア・モジュール１０及び２次（または受信）処理ソフトウェア・モジュール２０は、それぞれコンピュータ・システムの中央処理ユニット（ＣＰＵ）内で実行される。処理ユニット・ハードウェア装置３０（復号器など）が、コンピュータ・システムのバス２６の１つ上に存在する。基本ソフトウェア・モジュール１０と２次処理ソフトウェア・モジュール２０または処理ハードウェア３０との間の通信は、ＣＰＵ１１の外部に配置されるメモリ２５及びシステム・バス２６を介するデータ転送を要求する。基本ソフトウェア・モジュール１０は、データ処理モジュール２１及び暗号化モジュール２２を含む。データ処理モジュール２１は、データ・ストリームに対して実行される任意の通常の処理を含み、本発明によれば、受信された暗号化原始データ・ストリームの解読（ＣＳＳ解読など）を含む。２次処理ソフトウェア・モジュール２０は、解読モジュール２３及び処理モジュール２４を含み、処理ハードウェア装置３０は、解読装置２７及びデータ処理装置２８を含む。

【００１６】原始データは、例えば外部記憶装置またはコンピュータ・システム・ネットワークから、中央処理ユニット１１に到来する。このデータは、違法な複写から保護するために必要とされる部分を含み得る。この部分はここでは"著作権データ"と呼ばれ、それ自身を原始データから区別する。原始データ全体が保護される必要がある場合、著作権データは原始データと等価である。原始データは最初に基本ソフトウェア・モジュール１０の入力に転送され、データ処理モジュール２１により処理される。再度、例えばこれは、ＣＳＳ暗号化された原始データの解読ステップを含み得る。識別された著作権データが次に、暗号化モジュール２２により、異なる暗号化アルゴリズム、すなわちＣＳＳ暗号化以外の暗号化アルゴリズムを用いて再暗号化される。基本ソフトウェア・モジュール１０を通過する原始データは、非暗号化データ・ストリームまたは暗号化データ・ストリームを含み得る。第１のケースでは、データ処理モジュール２１が原始データを処理し、暗号化モジュール２２が暗号化アルゴリズムを実行し、著作権データを暗号化する。例えば暗号化アルゴリズムは、B. Schneierによる"Applied Cryptography"、John Wiley & Sons Inc. 、2nd Ed. (1996) で述べられるタイプである。

【００１７】第２のケースでは、データ処理モジュール２１が原始データを解読し、その後、暗号化モジュール２２がその著作権部分を前記同様の選択暗号化アルゴリズムを用いて再暗号化する。このプロシージャは、横断暗号化（trans-encryption）と呼ばれる。或いはデータ処理モジュール２１が原始データを解読しないように選択し、暗号化モジュール２２が元来暗号化された著作権データに加えて暗号化してもよい。このプロシージャは、層暗号化（layer-encryption）と呼ばれる。有利な点は、横断暗号化は、本発明に従いコンピュータ・システム内で使用される暗号化アルゴリズムが、原始データにより使用されるアルゴリズム、例えばＣＳＳ暗号化と異なることが可能な点である。層暗号化は、複数の暗号化アルゴリズムの使用を可能にし、それにより機密保護を強化する。

【００１８】暗号化された著作権データは、システム・メモリ２５またはシステム・バス２６の一方または両方を通じて転送され、究極的に２次処理ソフトウェア・モジュール２０または処理ハードウェア装置３０により受信される。上述のように、２次処理ソフトウェア・モジュール２０は、解読モジュール２３及びデータ処理モジュール２４を有し、処理ハードウェア装置３０は、解読装置２７及びデータ処理装置２８を含む。解読モジュール２３及び解読装置２７は、暗号化モジュール２２により暗号化されたデータを解読する。解読されたデータは次に、データ処理モジュール２４またはデータ処理装置２８により、それぞれ処理される。

【００１９】暗号化モジュール２２及び解読モジュール２３（または解読装置２７）により使用される暗号化／解読アルゴリズム対は、基本ソフトウェア・モジュール１０及び２次処理ソフトウェア・モジュール２０（または処理ハードウェア装置３０）の設計段階において、予

め定義されるデフォルトのアルゴリズム対である。或いは、アルゴリズム対がダウンロード可能なアルゴリズムであってもよい。

【００２０】例えば、暗号化モジュール２２に組み込まれる複数の暗号化アルゴリズム、及び解読モジュール２３または解読装置２７に組み込まれる複数の解読アルゴリズムが存在する。１つの適合対だけが任意の所与の時刻に使用される。暗号化に先立ち、暗号化モジュール２２は信号を解読モジュール２３または解読装置２７に送信し、それらに暗号化モジュール２２が使用する特定のアルゴリズムを知らせる。この信号はソフトウェア・パラメータ、或いはソフトウェアまたはハードウェア割込みの形式である。解読モジュール２３及び解読装置２７は、選択された暗号化／解読アルゴリズム対の対応する解読アルゴリズムを使用する。実際のアルゴリズムの内容は、モジュールまたは装置との間で伝送されないので、実際に使用される暗号化アルゴリズムは、ソフトウェア・モジュールまたはハードウェア装置内で逆エンジニアリングが実行されない限り、知られることはない。

【００２１】或いは、暗号化モジュール２２及び解読モジュール２３（または解読装置２７）が、設計段階において常駐型の暗号化／解読ルーチンを含むように事前定義され得る。暗号化に先立ち、暗号化モジュール２２は、使用する実際の暗号化及び解読アルゴリズム対を決定する。暗号化モジュール２２は常駐の暗号化アルゴリズムを用い、解読モジュール２３または解読装置２７により使用される選択アルゴリズム対の実際の解読ルーチンを暗号化する。暗号化モジュール２２は次に、実際の解読アルゴリズムの暗号化バージョンを解読モジュール２３または解読装置２７に伝送する。この情報の受信に際して、解読モジュール２３または解読装置２７は常駐の解読アルゴリズムを用い、ダウンロードされた解読アルゴリズムを解読する。解読モジュール２３は次に、解読された解読アルゴリズムをプロシージャ呼び出しとして使用し、一方、解読装置２７は解読アルゴリズムを自身内のプログラマブル回路にロードする。実際の解読アルゴリズムのダウンロードの完了の後、暗号化モジュール２２は実際の暗号化アルゴリズムを用いて、データを暗号化し、また解読モジュール２３または解読装置２７は、ダウンロードされた解読ルーチンを用いてデータを解読する。暗号化／解読ルーチンの更新が所望される場合、異なる暗号化／解読アルゴリズム対が選択され、暗号化モジュール２２が対応する解読アルゴリズムを解読モジュール２３または解読装置２７にダウンロードする。

【００２２】解読が実行された後、受信データ処理モジュール２４または装置２８が、生の圧縮ビデオ／音声データ信号のＭＰＥＧ復号などの、任意の要求データ処理を実行する。

【００２３】図２は、図１の装置を用いて、本発明に従いデータを保護する暗号化及び解読プロシージャを確立するための１実施例のフローチャートを示す。この処理フローは、原始データが基本ソフトウェア・モジュール１０（図１）に入力されるとき、開始される。最初に、基本ソフトウェア・モジュール１０が、受信データが保護される必要があるか否かを判断する（ステップ５０）。必要がない場合、暗号化モジュール２２がデータを直接、２次処理ソフトウェア・モジュール２０または処理ハードウェア装置３０に伝達する（ステップ６０）。例えば、ＤＶＤアプリケーションでは、基本ソフトウェア・モジュール１０は、複写生成管理システム（ＣＧＭＳ）データを調査することができる。受信データが保護される必要がある場合、次にステップ５１で、暗号化モジュール２２から解読モジュール２３または解読装置２７に、データの使用に先立ち解読が必要とされることを伝える。

【００２４】次に、処理は解読アルゴリズムがダウンロードされる必要があるか否かを判断する（ステップ５２）。必要ない場合、これはデフォルトの解読アルゴリズムが使用されることを意味し、処理は直接ステップ５４に移行する。それ以外では、ステップ５３で、アルゴリズムが解読モジュール２３または解読装置２７にダウンロードされる。

【００２５】解読アルゴリズムを確立した後、暗号化モジュール２２がキーを解読モジュール２３または解読装置２７に伝達し（ステップ５４）、キー及び暗号化アルゴリズムを用いて著作権データを暗号化する（ステップ５５）。暗号化キー及び暗号化データが、単一のビットストリームとして、または別々に、システム・メモリまたはシステム・バスの一方または両方を介して、解読モジュール２３または解読装置２７に送信される。ステップ５６で、解読モジュール２３または解読装置２７は、選択またはダウンロードされたアルゴリズムを用い、データを解読する。暗号化モジュール２２が次に、暗号化キーが更新されるべきか否かを判断する（ステップ５７）。更新されるべきでない場合、暗号化及び解読処理ステップ５５及び５６が繰り返される。要求に応じて同一の暗号化キーが、データ・ストリーム伝送の終りまで使用され得る。それ以外では、ステップ５４に戻り、新たな暗号化キーが解読モジュール２３または解読装置２７に伝達される。

【００２６】図３は、図２のステップ５４乃至５７に従い、暗号化キーを更新する装置／処理の１実施例を示す。暗号化モジュール２２内には、キー生成モジュール７９、キー暗号化モジュール８０、データ暗号化モジュール８１、及びデータ・マルチプレクサ・モジュール８２が含まれる。キー生成モジュール７９は原始キーを生成し、これはキー暗号化モジュール８０により暗号化され、またデータ暗号化モジュール８１によっても原始データを暗号化するために使用される。データ・マルチプ

レクサ８２は、暗号化されたキー及び暗号化データを１つのデータ・ストリームに結合し、これがメモリ及びシステム・バス８３を介して、解読モジュール２３または解読装置２７に伝送される。解読モジュール２３及び解読装置２７は、データ・デマルチプレクサ・モジュール／装置８４、キー解読モジュール／装置８５、及びデータ解読モジュール／装置８６を含む。データ・デマルチプレクサ・モジュール／装置８４は、受信されたデータ・ストリームを暗号化データ及び暗号化キーに結合解除する。キーが次に解読モジュール／装置８５により解読され、原始キーが生成される。データ解読モジュール８６は原始キーを用い、暗号化データを解読する。

【００２７】図４は更に、本発明に従う処理の１実施例を示す。この実施例では、ＣＳＳ解読の後、データ・ストリームが再暗号化され、復号器チップ内での伸長復号に先立ち、再暗号化されたストリームが解読される。図示の処理は、好適には１チップ・マイクロコード内で達成される。

【００２８】より詳細には、ビット・ストリームがＤＶＤディスク１００からホスト・プロセッサ１１０に読出され、ここで中央処理ユニットが認可されたＤＶＤキーを用いて、ＤＶＤ解読を実行する（１１２）。続く暗号化プロセスを保護するために、任意選択の不正防止（tamper resistance）アルゴリズム１１４が使用され得る。次に、生の暗号化ビット・ストリームが、任意の使用可能な暗号化／解読アルゴリズム、すなわちＣＳＳ符号化以外のアルゴリズムを用いて再暗号化される（１１６）。この再暗号化データは、例えばＭＰＥＧビデオ復号器１２８などの復号器に配送される。解読は対応するビット・ストリーム解読マイクロコードを含むマイクロコードのロード（１２４）に続いて、復号器１２８内で発生する。暗号化され、次に解読されるストリームの厳密な部分は使用されるアルゴリズムと同様、コードのリリース毎に変化し得る。データ・ストリームはＭＰＥＧビデオ・データ・ストリームを含み得、１実施例では、データ・ストリームがＤＶＤ解読処理１１２に続き、少なくとも部分的に再暗号化されるように、各ピクチャ１２０の１つ以上のフィールドが、ビット・ストリーム再暗号化処理１１６に従い暗号化される。解読キー１２２がマイクロコード・ロード１２４と同様、ビデオ・データ・ストリームと一緒に、ビデオ復号器１２８内のビット・ストリーム解読論理１２６に送信される。

【００２９】当業者であれば、上述の議論から、本発明によれば、（非圧縮のまたは圧縮された）生のデータが、ホスト・メモリ・バッファまたはシステム・バスなどの、アクセス可能なコンピュータ・システム構造内に決して存在せず、それにより生のデータの盗難を防止することが理解されよう。本発明は特に、デジタル・ビデオ・ディスク技術などにより使用される、ＭＰＥＧ符号化及びＣＳＳ符号化ビデオ・データに適用可能である。ここで提供される解読技術は、例えば解明され得る解読アルゴリズムの新たなマイクロコードをロードする柔軟性を通じて、続く変化を可能にする。更に、本発明の再暗号化技術により使用される特定の暗号化／解読アルゴリズムは変化し得る。概念的には、ホスト・ソフトウェアにより解読プロセスを開始し、中央処理ユニットにおいて異なる暗号化技術を用い、データを再暗号化し、受信モジュールにおいてデータの解読を完了する。その際、受信モジュールは、追加のソフトウェア・モジュールを含んでもよいし、或いは復号器などの受信ハードウェア装置を含んでもよい。受信された暗号化データの基本ソフトウェア解読に続く再暗号化は、完全であるかまたは部分的である。例えば、１実施例では、特定のＭＰＥＧデータがホスト・ソフトウェアにより暗号化される。ホストは次に、適切な解読マイクロコード・ロードまたは単一のマイクロコード・ロードを、適切なキーと共に受信モジュールまたは受信ハードウェア装置に送信する。受信モジュールにおいて、マイクロコードがホストにより使用される暗号化アルゴリズムの逆処理を実行する。キーは静的であるか、或いは累算され得る。

【００３０】更に当業者であれば、本発明が、例えばコンピュータ使用可能媒体を有する装置（例えば１つ以上のコンピュータ・プログラム製品）に含まれ得ることが理解されよう。組み込まれる媒体は、例えば、本発明の能力を提供及び容易にするコンピュータ読出し可能プログラム・コード手段である。本装置はコンピュータ・システムの一部として含まれるか、または別途販売される。

【００３１】ここで示されたフロー図は、一例として提供されたものである。本発明の趣旨から逸脱すること無しに、これらの図及びここで述べられたステップまたは操作に対する様々な変更が可能である。例えば、特定のケースでは、これらのステップが異なる順序で実行されたり、ステップが追加、消去または変更され得る。更に、ここでは主に、単一の基本モジュール、単一の受信処理モジュール、及び単一の処理ハードウェア装置に関して述べられたが、各タイプの複数のモジュール及びハードウェア装置が、本発明に従う装置として使用され得る。これらの全ての変更は、本発明の一部を成すものと見なされる。

【００３２】まとめとして、本発明の構成に関して以下の事項を開示する。

【００３３】（１）暗号化データ・ストリームを受信するように接続される中央処理ユニット（ＣＰＵ）を有するコンピュータ・システム内で、前記暗号化データ・ストリームを処理する装置であって、受信された前記暗号化データ・ストリームを解読し、生のデータ・ストリームを生成する前記ＣＰＵ内の第１の解読手段と、前記暗号化データ・ストリームとは異なる暗号化アルゴリズムにより、前記生のデータ・ストリームを再暗号化し、暗

号化データ・ストリームを生成する前記ＣＰＵ内の再暗号化手段と、前記暗号化データ・ストリームを前記ＣＰＵから、該ＣＰＵに接続される前記コンピュータ・システムの第２の構造に転送する手段と、前記第２の構造から前記暗号化データ・ストリームを受信し、該暗号化データ・ストリームを解読し、前記生のデータ・ストリームを生成する、前記第２の構造に接続される第２の解読手段とを含み、前記ＣＰＵ内の前記第１の解読手段が、受信された前記暗号化データ・ストリームの解読を実行する一方で、前記生のデータ・ストリームが、前記ＣＰＵから、該ＣＰＵに接続される前記第２の構造に転送される際に暴露されないようにする、装置。

（２）前記暗号化データ・ストリームが、暗号化された符号化データ・ストリームを含み、前記装置が、前記第２の解読手段により生成される生の符号化データ・ストリームを復号する、前記第２の解読手段に接続される復号器を含む、前記（１）記載の装置。

（３）前記生の符号化データ・ストリームがビデオ・データ・ストリームを含み、前記復号器がＭＰＥＧビデオ復号器を含む、前記（２）記載の装置。

（４）前記暗号化された符号化データ・ストリームが、ＣＳＳ暗号化されたＭＰＥＧ符号化データ・ストリームを含み、前記第１の解読手段が、前記暗号化された符号化データ・ストリームを前記ＣＰＵ内でＣＳＳ解読する手段を含み、前記復号器が前記生の符号化データ・ストリームをＭＰＥＧ復号する手段を含む、前記（２）記載の装置。

（５）前記復号器が復号ハードウェア装置を含み、前記第２の解読手段が前記復号ハードウェア装置内に存在する、前記（２）記載の装置。

（６）前記再暗号化手段が、前記生のデータ・ストリームを再暗号化するために使用されるキーを提供する手段を含み、前記第２の解読手段が前記キーを用いて、前記暗号化データ・ストリームを解読する手段を含む、前記（１）記載の装置。

（７）前記再暗号化手段が、前記キーを暗号化して暗号化キーを生成し、前記暗号化キー及び前記暗号化データ・ストリームを、前記ＣＰＵに接続される前記第２の構造への転送のために、多重化データ・ストリームに多重化する手段を含み、前記第２の解読手段が、前記多重化データ・ストリームを多重化解除し、前記暗号化キー及び前記暗号化データ・ストリームを獲得する手段と、前記暗号化キーを解読する手段とを含む、前記（６）記載の装置。

（８）前記再暗号化手段及び前記第２の解読手段により使用される暗号化／解読アルゴリズム対を選択する手段を含む、前記（１）記載の装置。

（９）前記選択手段が、選択された前記暗号化／解読アルゴリズム対の解読アルゴリズムを、前記再暗号化手段から前記第２の解読手段にダウンロードする手段を含み、前記ダウンロードする手段が、前記再暗号化手段と前記第２の解読手段との間の転送のために、前記解読アルゴリズムを暗号化する手段を含む、前記（８）記載の装置。

（１０）前記選択手段が、前記再暗号化手段及び前記第２の解読手段において、複数の暗号化／解読アルゴリズム対から、前記暗号化／解読アルゴリズム対を選択する手段を含み、前記選択手段が前記第２の解読手段に、前記複数の暗号化／解読アルゴリズム対の内で、前記再暗号化手段により使用される暗号化アルゴリズムに対応する解読アルゴリズムを知らせる手段を含む、前記（８）記載の装置。

（１１）前記第２の解読手段が前記ＣＰＵ内に配置される解読モジュールを含み、前記ＣＰＵに接続される前記第２の構造がメモリを含む、前記（１）記載の装置。

（１２）データ・ストリームを受信するように接続される中央処理ユニット（ＣＰＵ）を有するコンピュータ・システム内で、前記データ・ストリームを処理する装置であって、前記データ・ストリーム内で識別される著作権データを暗号化し、暗号化データを生成する、前記ＣＰＵ内の暗号化手段と、前記著作権データだけを前記暗号化データとして、前記ＣＰＵから、該ＣＰＵに接続される前記コンピュータ・システムの構造に転送する手段と、前記暗号化データを受信する前記構造に接続され、前記暗号化データを解読する手段を含む解読手段と、を含む、装置。

（１３）前記ＣＰＵ内で、前記データ・ストリームの前記著作権データを識別する手段を含み、該識別手段が識別された前記著作権データを前記暗号化手段に提供する、前記（１２）記載の装置。

（１４）前記データ・ストリームが暗号化された符号化データ・ストリームを含み、前記装置が、前記暗号化された符号化データ・ストリームを前記ＣＰＵ内で解読し、生の符号化データ・ストリームを生成する解読手段を含み、前記識別手段が前記生の符号化データ・ストリームを調査し、前記暗号化手段による暗号化のために著作権データを識別する、前記（１３）記載の装置。

（１５）前記解読手段がマイクロコード解読装置を含む、前記（１２）記載の装置。

（１６）前記データ・ストリームが暗号化データ・ストリームを含み、前記装置が、前記暗号化手段による、識別された前記著作権データの前記暗号化に先立ち、前記暗号化データ・ストリームを解読する手段を含み、前記暗号化データ・ストリームが、前記暗号化手段により生成される前記暗号化データとは異なる暗号化アルゴリズムから生成される、前記（１２）記載の装置。

（１７）前記暗号化手段が、識別された前記著作権データの前記暗号化において、及び前記解読手段による、前記暗号化データの解読のために使用されるキーを提供する手段を含む、前記（１２）記載の装置。

（１８）前記暗号化手段が前記キーを暗号化して暗号化キーを生成し、前記暗号化キー及び前記暗号化データを、前記ＣＰＵに接続される前記構造への転送のために、多重化データ・ストリームに多重化する手段を含み、前記解読手段が、前記多重化データ・ストリームを多重化解除し、前記暗号化キー及び前記暗号化データを獲得する手段と、前記暗号化キーを解読する手段とを含む、前記（１７）記載の装置。

（１９）複数の予め定義された暗号化／解読アルゴリズム対から、前記再暗号化手段及び前記解読手段により使用される暗号化／解読アルゴリズム対を選択する手段を含み、選択された前記暗号化／解読アルゴリズム対が、前記暗号化手段により使用される暗号化アルゴリズムと、前記解読手段により使用される対応する解読アルゴリズムとを含む、前記（１２）記載の装置。

（２０）中央処理ユニット（ＣＰＵ）及び該ＣＰＵに接続される構造を有するコンピュータ・システム内で、暗号化データ・ストリームを処理する方法であって、

ａ）前記ＣＰＵにおいて、前記暗号化データ・ストリームを受信するステップと、

ｂ）前記ＣＰＵ上で実行されるモジュール内で、前記暗号化データ・ストリームを解読し、生のデータを生成するステップと、

ｃ）前記生のデータを前記ＣＰＵ内で再暗号化し、少なくとも部分的に暗号化されたデータを生成するステップと、

ｄ）前記再暗号化に続き、前記少なくとも部分的に暗号化されたデータを、前記ＣＰＵから、該ＣＰＵに接続される前記コンピュータ・システムの第２の構造に転送するステップと、

ｅ）前記転送に続き、前記少なくとも部分的に暗号化されたデータを検索して解読し、生のデータを生成するステップと、

を含み、前記解読が前記ＣＰＵ上で実行される前記モジュール内で発生する一方で、前記生のデータが前記ＣＰＵから、該ＣＰＵに接続される前記構造に転送される際に、暴露されないようにし、前記暗号化データ・ストリームが、前記少なくとも部分的に暗号化されたデータを生成する前記再暗号化ステップｃ）により使用されるのとは異なる暗号化アルゴリズムから生成される、方法。

（２１）前記暗号化データ・ストリームが暗号化された符号化データ・ストリームを含み、前記解読ステップｅ）が生の符号化データを生成するステップを含み、前記方法が、前記生の符号化データを復号し、前記生のデータを生成するステップを含む、前記（２０）記載の方法。

（２２）前記暗号化された符号化データ・ストリームが、ＣＳＳ暗号化されたＭＰＥＧ符号化データ・ストリームを含み、前記解読ステップｂ）が、前記暗号化された符号化データ・ストリームを前記ＣＰＵ内でＣＳＳ解読するステップを含み、前記復号ステップが、前記生の符号化データをＭＰＥＧ復号し、前記生のデータを生成するステップを含む、前記（２１）記載の方法。

（２３）前記再暗号化ステップｃ）が、キーを用いて前記生のデータを暗号化するステップを含み、前記方法が、前記解読ステップｅ）のために前記キーを提供するステップを含み、前記解読ステップが前記キーを用いて、前記少なくとも部分的に暗号化されたデータを解読する、前記（２０）記載の方法。

（２４）前記再暗号化ステップｃ）が、前記キーを暗号化して暗号化キーを生成し、前記暗号化キー及び前記少なくとも部分的に暗号化されたデータを多重化データ・ストリームに多重化するステップを含み、前記解読ステップｅ）が、前記多重化データ・ストリームを多重化解除し、前記暗号化キー及び前記少なくとも部分的に暗号化されたデータを獲得するステップと、前記暗号化キーを解読し、前記キーを用いて、前記少なくとも部分的に暗号化されたデータを解読するステップとを含む、前記（２３）記載の方法。

（２５）複数の予め定義された暗号化／解読アルゴリズム対から、前記再暗号化ステップｃ）及び前記解読ステップｅ）により使用される暗号化／解読アルゴリズム対を選択するステップを含む、前記（２０）記載の方法。

（２６）前記再暗号化ステップｃ）が前記選択ステップを実行し、前記再暗号化ステップが、前記解読ステップｅ）により使用される前記暗号化／解読アルゴリズム対の解読アルゴリズムをダウンロードするステップを含む、前記（２５）記載の方法。

（２７）前記解読ステップｅ）が、前記少なくとも部分的に暗号化されたデータを前記ＣＰＵ内で解読するステップを含み、前記ＣＰＵに接続される前記構造がメモリ構造を含み、前記検索ステップｅ）が、前記メモリ構造から、前記少なくとも部分的に暗号化されたデータを検索するステップを含む、前記（２０）記載の方法。

（２８）中央処理ユニット（ＣＰＵ）と、該ＣＰＵの外部にあって該ＣＰＵに接続される構造とを有するコンピュータ・システム内で、データ・ストリームを処理する方法であって、

ａ）前記ＣＰＵにおいて、前記データ・ストリームを受信するステップと、

ｂ）前記データ・ストリーム内で識別される著作権データを暗号化し、暗号化データを生成するステップと、

ｃ）前記暗号化ステップｂ）に続き、前記著作権データだけを前記暗号化データとして、前記ＣＰＵから該ＣＰＵに接続される構造に転送するステップと、

ｄ）前記ＣＰＵに接続される前記構造から前記暗号化データを検索し、該暗号化データを解読して、生のデータを生成するステップと、を含み、前記解読ステップが、前記暗号化データを前記ＣＰＵの外部の前記構造へ転送した後に発生し、前記生のデータが、前記ＣＰＵと該Ｃ

ＰＵに接続される前記構造との間で転送される際に、前記コンピュータ・システム内で暴露されないようにする、方法。

（２９）前記暗号化ステップｂ）により使用される前記データ・ストリームの前記著作権データを、前記ＣＰＵ内で識別するステップを含む、前記（２８）記載の方法。

（３０）前記データ・ストリームが暗号化データ・ストリームを含み、前記方法が、前記著作権データの前記識別に先立ち、前記暗号化データ・ストリームを解読するステップを含み、前記暗号化データ・ストリームが、前記暗号化ステップｂ）により使用されるのとは異なる暗号化アルゴリズムから生成される、前記（２９）記載の方法。

（３１）前記暗号化ステップｂ）が、識別された前記著作権データをキーを用いて暗号化し、前記キーを前記解読ステップｄ）に提供するステップを含む、前記（２８）記載の方法。

（３２）前記暗号化ステップｂ）が前記キーを暗号化して暗号化キーを生成し、前記暗号化キー及び前記暗号化データを、前記ＣＰＵに接続される前記構造への転送のために、多重化データ・ストリームに多重化するステップを含み、前記解読ステップｄ）が、前記多重化データ・ストリームを多重化解除し、前記暗号化キー及び前記暗号化データを獲得するステップと、前記暗号化データの解読のために使用する前記暗号化キーを解読するステップとを含む、前記（３１）記載の方法。

（３３）複数の予め定義された暗号化／解読アルゴリズム対から、暗号化／解読アルゴリズム対を選択するステップを含み、前記暗号化ステップｂ）が、選択された前記暗号化／解読アルゴリズム対の暗号化アルゴリズムを用いて、識別された前記著作権データを暗号化し、前記解読ステップｄ）が、選択された前記暗号化／解読アルゴリズム対の対応する解読アルゴリズムを用い、前記暗号化データを解読するステップを含む、前記（２８）記載の方法。

（３４）中央処理ユニット（ＣＰＵ）及び該ユニットに接続される構造を有するコンピュータ・システム内で、暗号化データ・ストリームを処理するために使用されるコンピュータ読出し可能プログラム・コード手段を有するコンピュータ使用可能媒体を含むコンピュータ・プログラム製品であって、前記ＣＰＵにおいて前記暗号化データ・ストリームを受信し、前記ＣＰＵ内で前記暗号化データ・ストリームを解読し、生のデータを生成し、該生のデータを前記ＣＰＵ内で再暗号化し、少なくとも部分的に暗号化されたデータを生成する、コンピュータ読出し可能プログラム・コード手段と、前記少なくとも部分的に暗号化されたデータを、前記ＣＰＵから該ＣＰＵに接続される前記構造に転送する、コンピュータ読出し可能プログラム・コード手段と、前記ＣＰＵに接続される前記構造から、前記少なくとも部分的に暗号化されたデータを検索し、前記少なくとも部分的に暗号化されたデータを解読して、生のデータを生成する、コンピュータ読出し可能プログラム・コード手段とを含み、前記解読が前記ＣＰＵ内で発生する一方で、前記生のデータが、前記ＣＰＵから該ＣＰＵに接続される前記構造に転送される際に、暴露されないようにする、コンピュータ・プログラム製品。

（３５）前記暗号化データ・ストリームが、暗号化された符号化データ・ストリームを含み、前記コンピュータ・プログラム製品が、前記少なくとも部分的に暗号化されたデータを解読する前記コンピュータ読出し可能プログラム・コード手段により生成された生の符号化データを復号する、コンピュータ読出し可能プログラム・コード手段を含む、前記（３４）記載のコンピュータ・プログラム製品。

（３６）前記暗号化された符号化データ・ストリームが、ＣＳＳ暗号化されたＭＰＥＧ符号化データ・ストリームを含み、前記暗号化された符号化データ・ストリームを解読する前記コンピュータ読出し可能コード手段が、前記暗号化された符号化データ・ストリームをＣＳＳ解読するコンピュータ読出し可能プログラム・コード手段を含み、前記復号のためのコンピュータ読出し可能プログラム・コード手段が、前記生の符号化データ・ストリームをＭＰＥＧ復号するコンピュータ読出し可能プログラム・コード手段を含む、前記（３５）記載のコンピュータ・プログラム製品。

（３７）中央処理ユニット（ＣＰＵ）と、該ＣＰＵの外部にあって該ＣＰＵに接続される構造とを有するコンピュータ・システム内で、データ・ストリームを処理するために使用されるコンピュータ読出し可能プログラム・コード手段を有するコンピュータ使用可能媒体を含むコンピュータ・プログラム製品であって、前記ＣＰＵにおいて前記データ・ストリームを受信し、該データ・ストリーム内で識別される著作権データを暗号化し、暗号化データを生成する、コンピュータ読出し可能プログラム・コード手段と、前記暗号化データを、前記ＣＰＵから該ＣＰＵの外部の前記構造に転送する、コンピュータ読出し可能プログラム・コード手段と、前記ＣＰＵの外部の前記構造への転送の後、前記暗号化データを検索して解読する、コンピュータ読出し可能プログラム・コード手段と、を含み、前記生のデータが、前記ＣＰＵと該ＣＰＵに接続される前記構造との間の転送に際し、前記コンピュータ・システム内で暴露されないようにする、コンピュータ・プログラム製品。

（３８）前記データ・ストリームの前記著作権データを識別して暗号化する、コンピュータ読出し可能プログラム・コード手段を含む、前記（３７）記載のコンピュータ・プログラム製品。

（３９）識別された前記著作権データを暗号化する前記

コンピュータ読出し可能プログラム・コード手段が、キーを用いて前記暗号化を実行し、前記キーを前記暗号化データを解読する前記コンピュータ読出し可能プログラム・コード手段に提供する、コンピュータ読出し可能プログラム・コード手段を含む、前記（３７）記載のコンピュータ・プログラム製品。

（４０）前記暗号化のためのコンピュータ読出し可能プログラム・コード手段が、前記キーを暗号化して、暗号化キーを生成し、前記暗号化キー及び前記暗号化データを、前記ＣＰＵに接続される前記構造への転送のために、多重化データ・ストリームに多重化するコンピュータ読出し可能プログラム・コード手段を含み、前記解読のためのコンピュータ読出し可能プログラム・コード手段が、前記多重化データ・ストリームを多重化解除し、前記暗号化キー及び前記暗号化データを獲得し、前記暗号化データの解読のために使用する前記暗号化キーを解読するコンピュータ読出し可能プログラム・コード手段を含む、前記（３９）記載のコンピュータ・プログラム製品。

（４１）識別された前記著作権データの暗号化、及び前記暗号化データの解読において使用される暗号化／解読アルゴリズム対を、複数の予め定義された暗号化／解読アルゴリズム対から選択するコンピュータ読出し可能プログラム・コード手段を含み、前記暗号化データを解読する前記コンピュータ読出し可能プログラム・コード手段に、選択された前記暗号化／解読アルゴリズム対の対応する解読アルゴリズムを知らせる、コンピュータ読出し可能プログラム・コード手段を含む、前記（３７）記載のコンピュータ・プログラム製品。

【図面の簡単な説明】

【図１】本発明に従う暗号化／解読装置を使用するコンピュータ・システムの１実施例を示す図である。

【図２】本発明に従う暗号化／解読処理を実行する１実施例のフローチャートである。

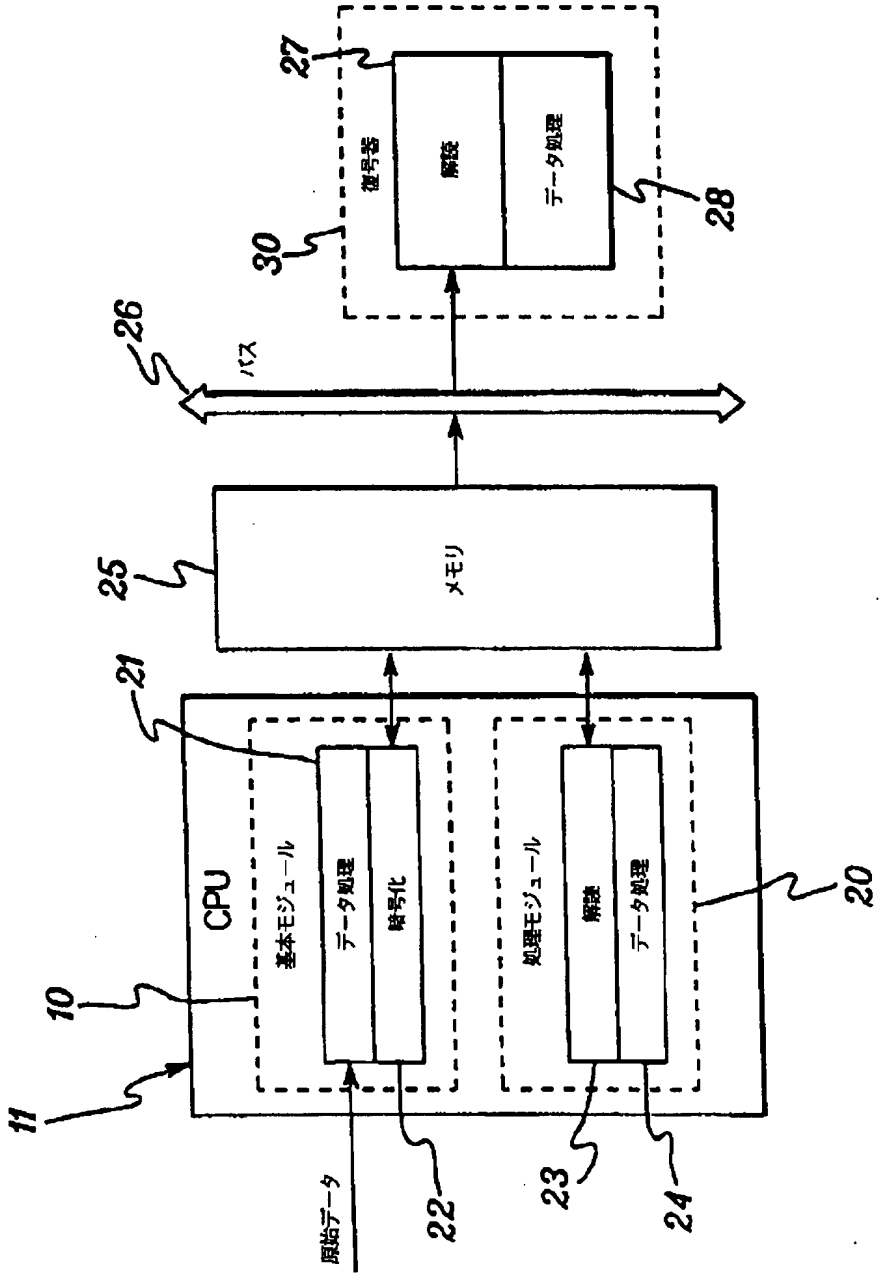
【図３】本発明に従う装置の暗号化及び解読モジュール及び（または）機構内の、キーを更新する１実施例のブロック図である。

【図４】本発明に従い、マイクロコードを用いるＤＶＤディスク・データ・ストリーム処理の１実施例を表す図である。

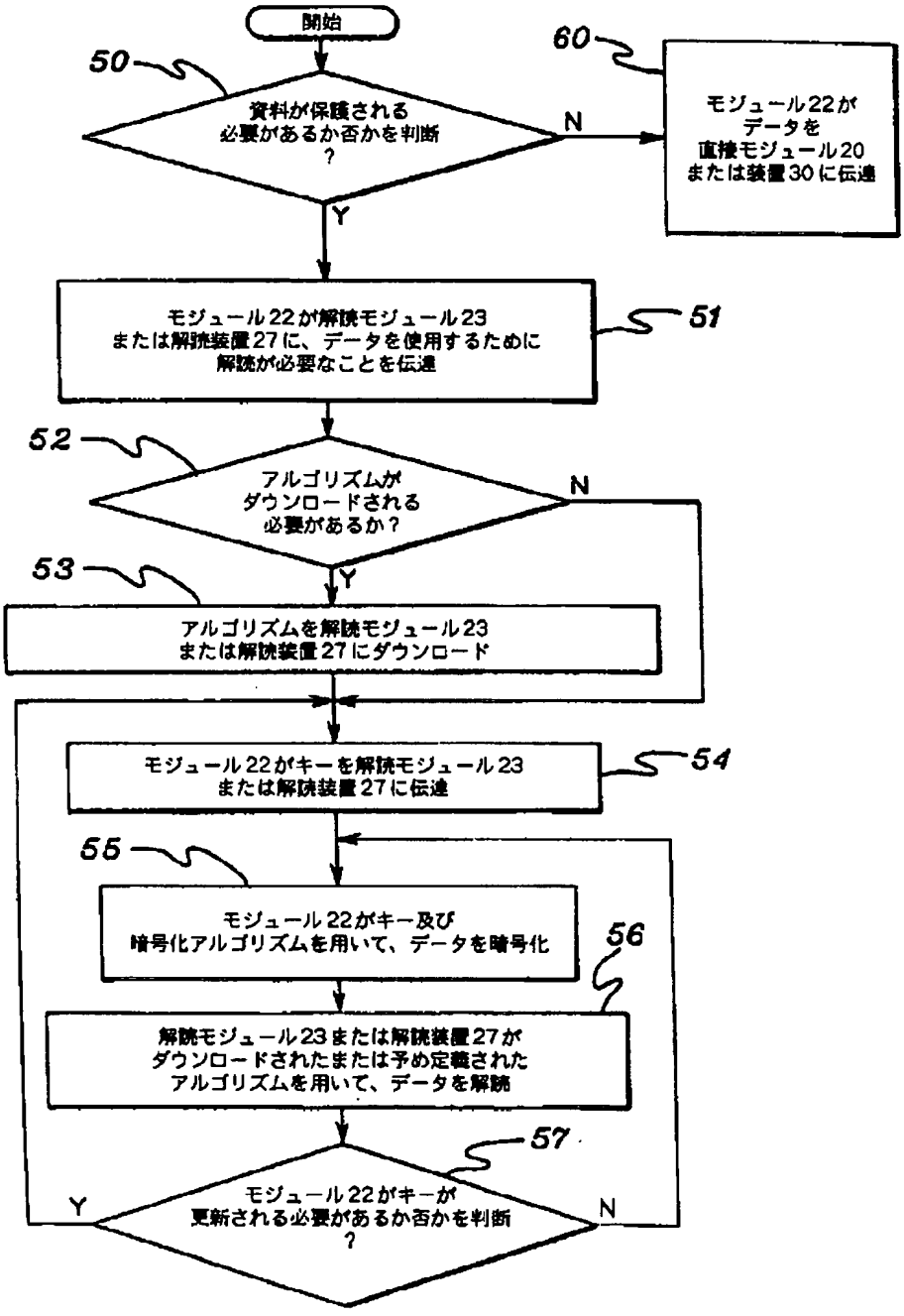
【符号の説明】

１０　基本ソフトウェア・モジュール
１１　ＣＰＵ
２０　２次（または受信）処理ソフトウェア・モジュール
２１　データ処理モジュール
２２　暗号化モジュール
２３　解読モジュール
２４　処理モジュール
２５　メモリ
２６、８３　システム・バス
２７　解読装置
２８　データ処理装置
３０　処理ユニット・ハードウェア装置
７９　キー生成モジュール
８０　キー暗号化モジュール
８１　データ暗号化モジュール
８２　データ・マルチプレクサ・モジュール
８４　データ・デマルチプレクサ・モジュール／装置
８５　キー解読モジュール／装置
８６　データ解読モジュール／装置
１００　ＤＶＤディスク
１１０　ホスト・プロセッサ
１１２　ＤＶＤ解読処理
１１４　不正防止（tamper resistance）アルゴリズム
１１６　ビット・ストリーム再暗号化処理
１２０　ピクチャ
１２２　解読キー
１２４　マイクロコード・ロード
１２６　ビット・ストリーム解読論理
１２８　ＭＰＥＧビデオ復号器

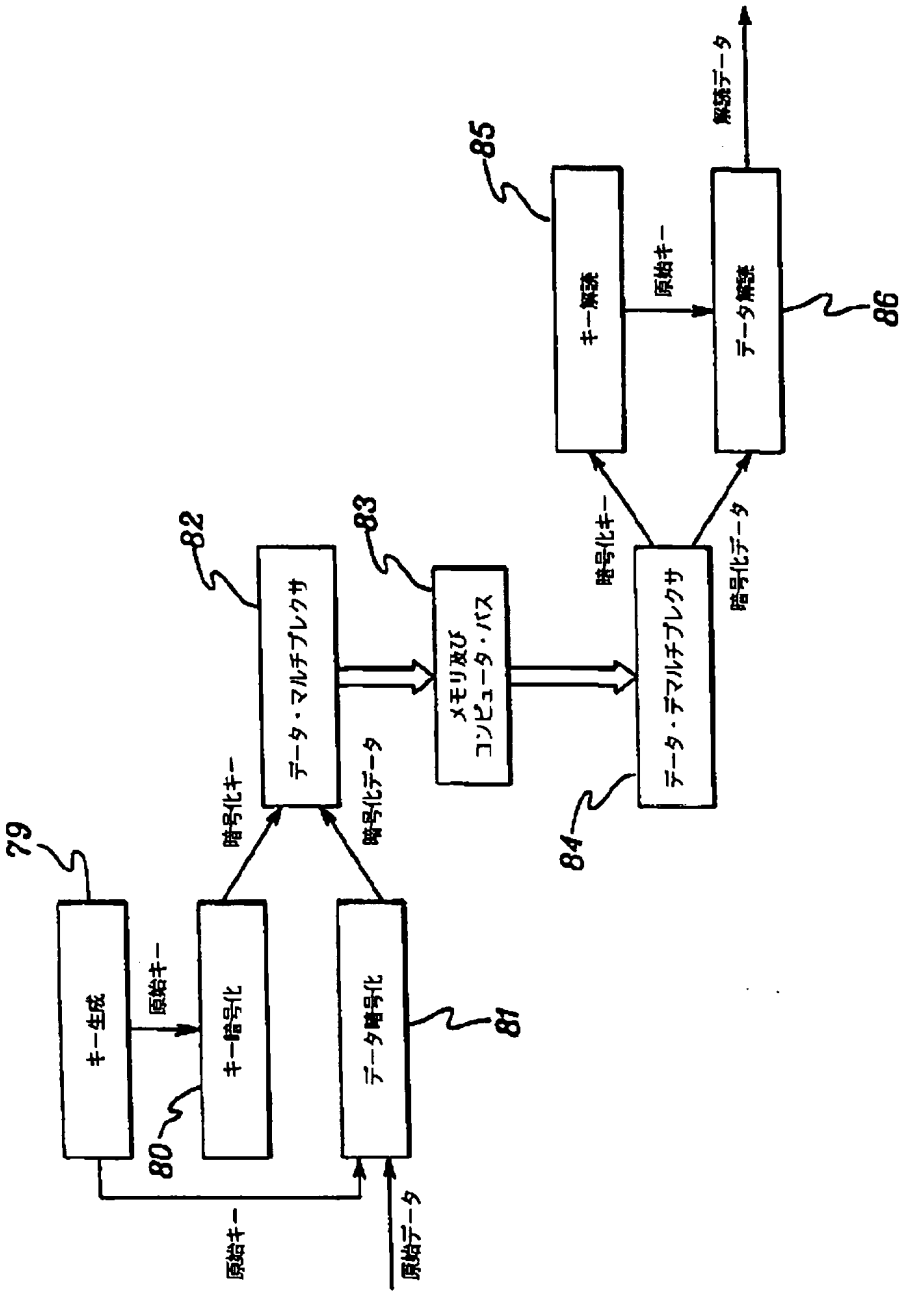
【図１】


27
復号器
解読
データ処理
28
30
26
バス
25
メモリ
21
CPU
基本モジュール
データ処理
暗号化
処理モジュール
解読
データ処理
20
10
11
原始データ
22
23
24

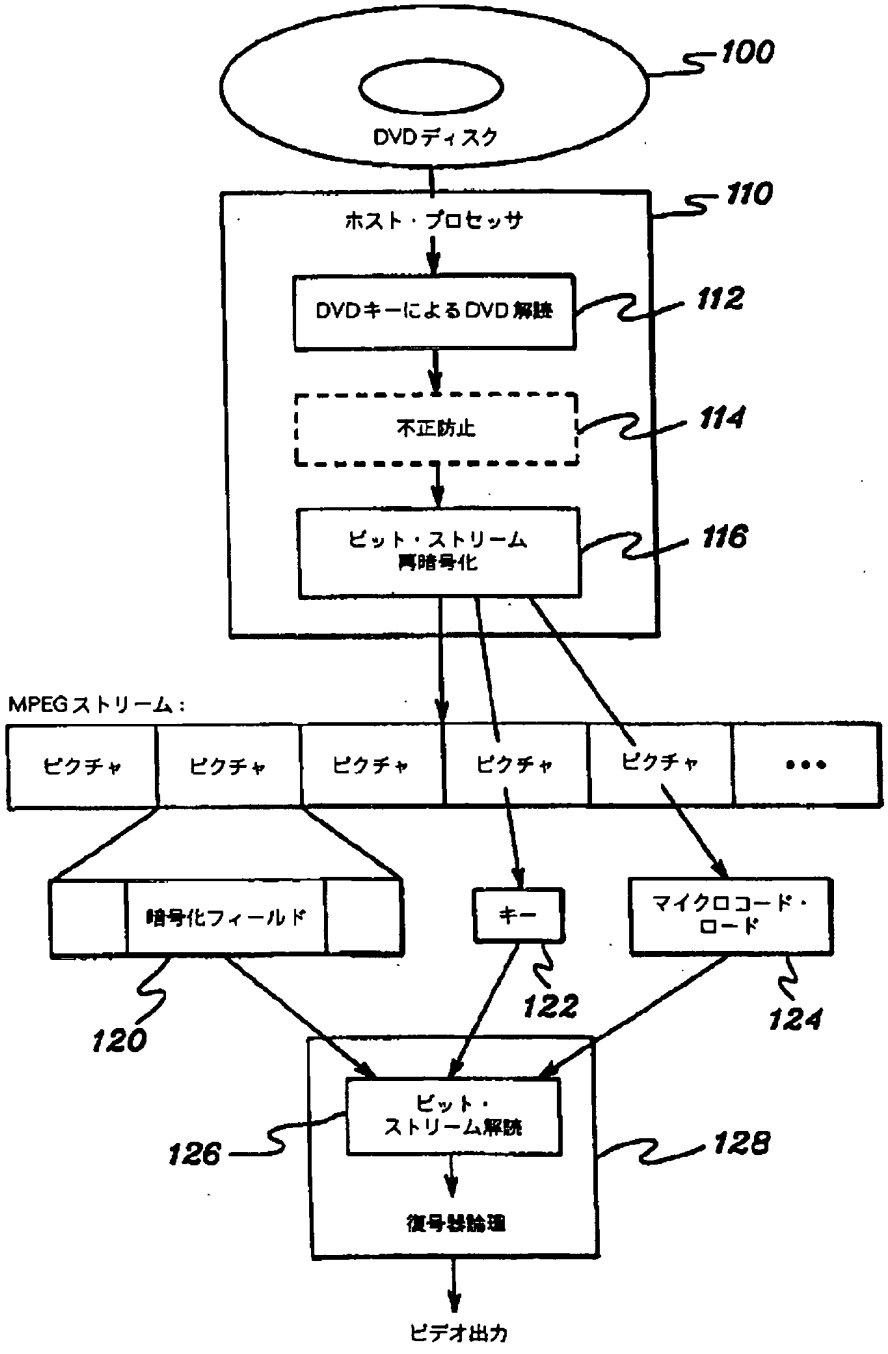
【図２】


開始
50
資料が保護される必要があるか否かを判断？
N
60
モジュール22がデータを直接モジュール20または装置30に伝達
Y
モジュール22が解読モジュール23または解読装置27に、データを使用するために解読が必要なことを伝達
51
52
アルゴリズムがダウンロードされる必要があるか？
N
Y
53
アルゴリズムを解読モジュール23または解読装置27にダウンロード
モジュール22がキーを解読モジュール23または解読装置27に伝達
54
55
モジュール22がキー及び暗号化アルゴリズムを用いて、データを暗号化
56
解読モジュール23または解読装置27がダウンロードされたまたは予め定義されたアルゴリズムを用いて、データを解読
57
モジュール22がキーが更新される必要があるか否かを判断？
Y
N

【図３】


79
キー生成
原始キー
80
キー暗号化
暗号化キー
82
データ・マルチプレクサ
83
メモリ及び
コンピュータ・バス
暗号化キー
暗号化データ
84
データ・デマルチプレクサ
85
キー解読
原始キー
データ解読
86
解読データ
データ暗号化
81
暗号化データ
原始キー
原始データ

【図４】



フロントページの続き

(72)発明者　ジョン・ウィリアム・ウルダ
アメリカ合衆国13760、ニューヨーク州エンドウェル、パーク・ヒル・ドライブ
1007

(72)発明者　ワイ・マン・ラム
アメリカ合衆国10547、ニューヨーク州モヒガン・レイク、サニー・リッジ・ロード
1325

(72)発明者　ジャック・ローレンス・コーロヘリス
アメリカ合衆国10562、ニューヨーク州オシニング、スノーデン・アベニュー　46

(72)発明者　ジョン・エドワード・フェッコビッチ
アメリカ合衆国13760、ニューヨーク州エンディコット、リバー・テラス　427、アパートメント　エフー３

【外国語明細書】

1. Title of Invention

APPARATUS, METHOD AND COMPUTER PROGRAM PRODUCT FOR PROTECTING COPYRIGHT DATA WITHIN A COMPUTER SYSTEM

2. Claims

(1) Apparatus for processing a scrambled data stream within a computer system having a central processing unit (CPU) coupled to receive the scrambled data stream, comprising:

descrambling means within the central processing unit for descrambling the received, scrambled data stream to produce a clear data stream;

re-encryption means within the central processing unit for re-encrypting the clear data stream to produce an encrypted data stream, wherein said scrambled data stream is produced from a different encryption algorithm than said encrypted data stream;

means for transferring the encrypted data stream from the central processing unit to a second structure of the computer system, said second structure being coupled to the CPU; and

decryption means coupled to the second structure for receiving the encrypted data stream therefrom and for decrypting the encrypted data stream to produce said clear data stream, wherein said clear data stream is unexposed when transferred from the central processing unit to said second structure coupled to the CPU, while said descrambling means within the central processing unit accomplishes descrambling of the received scrambled data stream.

(2) The apparatus of claim 1, wherein said scrambled data stream comprises a scrambled, encoded data stream and wherein said apparatus further comprises a decoder coupled to said decryption means for decoding a clear, encoded data stream produced by said decryption means.

(3) The apparatus of claim 2, wherein said clear, encoded data stream comprises a video data stream and wherein said decoder comprises an MPEG video decoder.

(4) The apparatus of claim 2, wherein said scrambled, encoded data stream comprises a CSS scrambled, MPEG encoded data stream, and wherein said descrambling means comprises means for CSS

descrambling the scrambled, encoded data stream within the CPU and said decoder comprises means for MPEG decoding said clear, encoded data stream.

(5) The apparatus of claim 2, wherein said decoder comprises a decoding hardware device and said decryption means resides within said decoding hardware device.

(6) The apparatus of claim 1, wherein said re-encryption means further comprises means for providing a key for use in re-encrypting the clear data stream, and wherein said decryption means includes means for employing the key in decrypting the encrypted data stream.

(7) The apparatus of claim 6, wherein said re-encryption means further comprises means for encrypting said key to produce an encrypted key, and for multiplexing the encrypted key and the encrypted data stream into a multiplexed data stream for transfer to said second structure coupled to the CPU, and wherein said decryption means further comprises means for demultiplexing said multiplexed data stream to obtain said encrypted key and said encrypted data stream, and wherein said decryption means further comprises means for decrypting said encrypted key.

(8) The apparatus of claim 1, further

comprising means for selecting an encryption/decryption algorithm pair for use by said re-encryption means and said decryption means.

(9) The apparatus of claim 8, wherein said means for selecting comprises means for downloading a decryption algorithm of said selected encryption/decryption algorithm pair from said re-encryption means to said decryption means, said means for downloading including means for encrypting the decryption algorithm for transfer between the re-encryption means and the decryption means.

(10) The apparatus of claim 8, wherein said means for selecting comprises means for selecting said encryption/decryption algorithm pair from a plurality of encryption/decryption algorithm pairs at said re-encryption means and said decryption means, and wherein said means for selecting comprises means for noticing the decryption means which decryption algorithm of said plurality of encryption/decryption algorithm pairs corresponds with an encryption algorithm employed by said re-encryption means.

(11) The apparatus of claim 1, wherein said decryption means comprises a decryption module disposed within the central processing unit, and said second structure coupled to the CPU comprises memory.

(12) Apparatus for processing a data stream within a computer system having a central processing unit (CPU) coupled to receive the data stream, said apparatus comprising:

encryption means within the CPU for encrypting identified copyright data within the data stream to produce therefrom encrypted data;

means for transferring the encrypted data from the central processing unit to a structure of the computer system coupled thereto, wherein said copyright data is only transferred from the central processing unit as said encrypted data; and

decryption means coupled to said structure receiving the encrypted data, said decryption means comprising means for decrypting the encrypted data.

(13) The apparatus of claim 12, further comprising means for identifying within the central processing unit said copyright data of the data stream, said means for identifying providing said identified copyright data to said encryption means.

(14) The apparatus of claim 13, wherein the data stream comprises a scrambled, encoded data stream.

and wherein said apparatus further comprises descrambling means for descrambling the scrambled, encoded data stream within the central processing unit to produce a clear, encoded data stream, and wherein said means for identifying comprises means for examining the clear, encoded data stream to identify copyright data for encryption by said encryption means.

(15) The apparatus of claim 12, wherein said decryption means comprises a microcode decryption device.

(16) The apparatus of claim 12, wherein said data stream comprises a scrambled data stream, and wherein said apparatus further comprises means for descrambling the scrambled data stream prior to said encrypting of the identified copyright data by said encryption means, wherein said scrambled data stream is produced from a different encryption algorithm than said encrypted data produced by said encryption means.

(17) The apparatus of claim 12, wherein said encryption means further comprises means for providing a key for use in said encrypting of the identified copyright data and for use by said decryption means for decrypting the encrypted data.

(18) The apparatus of claim 17, wherein said encryption means further comprises means for encrypting said key to produce an encrypted key, and for multiplexing the encrypted key and the encrypted data into a multiplexed data stream for transfer to said structure coupled to the CPU, and wherein said decryption means further comprises means for demultiplexing said multiplexed data stream to obtain said encrypted key and said encrypted data, and wherein said decryption means further comprises means for decrypting said encrypted key.

(19) The apparatus of claim 12, further comprising means for selecting an encryption/decryption algorithm pair for use by said encryption means and said decryption means from a plurality of predefined encryption/decryption algorithm pairs, said selected encryption/decryption algorithm pair comprising an encryption algorithm and a corresponding decryption algorithm, said encryption algorithm being employed by said encryption means, and said corresponding decryption algorithm being employed by said decryption means.

(20) A method for processing a scrambled data stream within a computer system having a central processing unit and a structure coupled thereto, said

method comprising:

(a) receiving the scrambled data stream at the central processing unit (CPU);

(b) descrambling the scrambled data stream within a module executing on the central processing unit to produce clear data;

(c) re-encrypting the clear data within the central processing unit, said re-encrypting producing at least partially encrypted data;

(d) subsequent to said re-encrypting, transferring the at least partially encrypted data from the central processing unit to a second structure of the computer system, said second structure being coupled to the central processing unit; and

(e) subsequent to said transferring, retrieving and decrypting the at least partially encrypted data to produce clear data, wherein said clear data is unexposed when transferred from the central processing unit to the structure coupled thereto, while said descrambling occurs within the module executing on the central processing unit, and wherein the scrambled data stream is produced from a

different encryption algorithm than employed by said re-encrypting (c) to produce said at least partially encrypted data.

(21) The method of claim 20, wherein the scrambled data stream comprises a scrambled, encoded data stream, and wherein said decrypting (e) comprises producing clear, encoded data, and wherein said method further comprises decoding said clear, encoded data to produce said clear data.

(22) The method of claim 21, wherein said scrambled, encoded data stream comprises a CSS scrambled, MPEG encoded data stream, and wherein said descrambling (b) comprises CSS descrambling said scrambled, encoded data stream within the CPU, and said decoding comprises MPEG decoding said clear, encoded data to produce said clear data.

(23) The method of claim 20, wherein said re-encrypting (c) includes employing a key in re-encrypting the clear data, and wherein said method further comprises providing said key for said decrypting (e), said decrypting employing said key in decrypting the at least partially encrypted data.

(24) The method of claim 23, wherein said re-encrypting (c) includes encrypting said key to

produce an encrypted key, and multiplexing the encrypted key and the at least partially encrypted data into a multiplexed data stream, and wherein said decrypting (e) further comprises demultiplexing said multiplexed data stream to obtain said encrypted key and said at least partially encrypted data, and said decrypting (c) further comprises decrypting said encrypted key and employing said key in decrypting said at least partially encrypted data.

(25) The method of claim 20, further comprising selecting an encryption/decryption algorithm pair for use by said re-encrypting (c) and said decrypting (e), said selecting comprising choosing said selected encryption/decryption algorithm pair from a plurality of predefined encryption/decryption algorithm pairs.

(26) The method of claim 25, wherein said re-encrypting (c) accomplishes said selecting and said re-encrypting further comprises downloading a decryption algorithm of the selected encryption/decryption algorithm pair for use by said decrypting (c).

(27) The method of claim 20, wherein said decrypting (e) comprises decrypting the at least partially encrypted data within the central processing unit, and wherein said structure coupled to the central processing unit comprises a memory

structure, said retrieving (e) comprising retrieving said at least partially encrypted data from said memory structure.

(28) A method for processing a data stream within a computer system having a central processing unit and a structure outside the central processing unit coupled thereto, said method comprising:

(a) receiving the data stream at the central processing unit (CPU);

(b) encrypting identified copyright data within the data stream to produce encrypted data;

(c) subsequent to said encrypting (b), transferring the encrypted data from the central processing unit to the structure coupled thereto, wherein said copyright data is only transferred from the central processing unit as said encrypted data; and

(d) retrieving the encrypted data from the structure coupled to the CPU and decrypting the encrypted data to produce clear data, said decrypting occurring after transfer of the encrypted data to the structure outside the central processing unit, wherein said clear data

is unexposed within the computer system when transferred between the central processing unit and the structure coupled thereto.

(29) The method of claim 28, further comprising identifying within the central processing unit said copyright data of the data stream for use by said encrypting (b).

(30) The method of claim 29, wherein said data stream comprises a scrambled data stream, and said method further comprises descrambling the scrambled data stream prior to said identifying of the copyright data, and wherein said scrambled data stream is produced from a different encryption algorithm than employed by said encrypting (b).

(31) The method of claim 28, wherein said encrypting (b) includes employing a key in encrypting said identified copyright data and providing said key to said decrypting (d).

(32) The method of claim 31, wherein said encrypting (b) further comprises encrypting said key to produce an encrypted key, and multiplexing the encrypted key and the encrypted data into a multiplexed data stream for transfer to said structure coupled to the CPU, and wherein said decrypting (d) further comprises demultiplexing said

multiplexed data stream to obtain said encrypted key and said encrypted data, and wherein said decrypting (d) further comprises decrypting said encrypted key for use in decrypting said encrypted data.

(33) The method of claim 28, further comprising selecting an encryption/decryption algorithm pair from a plurality of predefined encryption/decryption algorithm pairs, and wherein said encrypting (b) comprises employing an encryption algorithm of said selected encryption/decryption algorithm pair in encrypting said identified copyright data, and said decrypting (d) comprises employing a corresponding decryption algorithm of said selected encryption/decryption algorithm pair for use in decrypting the encrypted data.

(34) A computer program producing comprising a computer usable medium having computer readable program code means therein for use in processing a scrambled data stream within a computer system having a central processing unit and a structure coupled thereto, said computer readable program code means in said computer program product comprising:

computer readable program code means for causing a computer to affect receiving of the scrambled data stream at the central processing unit and for descrambling the scrambled data

stream within the central processing unit to produce clear data, and for re-encrypting the clear data within the central processing unit to produce at least partially encrypted data;

computer readable program code means for causing a computer to affect transferring of said at least partially encrypted data from the central processing unit to the structure coupled thereto; and

computer readable program code means for causing a computer to affect retrieving of the at least partially encrypted data from the structure coupled to the CPU and for decrypting the at least partially encrypted data, said decrypting producing clear data, wherein said clear data is unexposed when transferred from the central processing unit to the structure coupled thereto, while said descrambling occurs within the central processing unit.

(35) The computer readable program code means of claim 34, wherein the scrambled data stream comprises a scrambled, encoded data stream, and wherein said computer readable program code means in said computer program product further comprises computer readable program code means for causing a computer to affect decoding of clear, encoded data produced by said

computer readable program code means for decrypting the at least partially encrypted data.

(36) The computer readable program code means of claim 35, wherein said scrambled, encoded data stream comprises a CSS scrambled, MPEG encoded data stream and wherein said computer readable code means for descrambling said scrambled, encoded data stream comprises computer readable program code means for causing a computer to affect CSS descrambling of the scrambled, encoded data stream, and wherein said computer readable program code means for decoding comprises computer readable program code means for causing a computer to affect MPEG decoding of said clear, encoded data stream.

(37) A computer program product comprising a computer useable medium having computer readable program code means therein for use in processing a data stream within a computer system having a central processing unit and a structure outside the central processing unit coupled thereto, said computer readable program code means in said computer program product comprising:

computer readable program code means for causing a computer to affect receiving of the data stream at the central processing unit and encrypting of identified copyright data within

the data stream to produce encrypted data;

computer readable program code means for causing a computer to affect transferring of the encrypted data from the central processing unit to the structure outside the central processing unit; and

computer readable program code means for causing a computer to affect retrieving and decrypting of the encrypted data after transfer to the structure outside the central processing unit, wherein clear data is unexposed within the computer system when transferred between the central processing unit and the structure coupled thereto.

(38) The computer readable program code means of claim 37, further comprising computer readable program code means for causing a computer to affect identifying said copyright data of the data stream for encrypting.

(39) The computer readable program code means of claim 37, wherein said computer readable program code means for encrypting the identified copyright data includes computer readable program code means for causing a computer to affect said encrypting using a key and for providing said key to said computer

readable program code means for decrypting the encrypted data.

(40) The computer readable program code means of claim 39, wherein said computer readable program code means for encrypting comprises computer readable program code means for causing a computer to affect encrypting of said key to produce an encrypted key, and for multiplexing the encrypted key and the encrypted data into a multiplexed data stream for transfer to said structure coupled to the CPU, and wherein said computer readable program code means for decrypting comprises computer readable program code means for causing a computer to affect demultiplexing of the multiplexed data stream to obtain said encrypted key and said encrypted data, and for decrypting the encrypted key for use in decrypting the encrypted data.

(41) The computer readable program code means of claim 37, further comprising computer readable program code means for causing a computer to affect selecting an encryption/decryption algorithm pair for use in encrypting said identified copyright data and decrypting said encrypted data, said selected encryption/decryption algorithm pair being selected from a plurality of predefined encryption/decryption algorithm pairs, and further comprising computer

readable program code means for causing a computer to affect noticing of a corresponding decryption algorithm of the selected encryption/decryption algorithm pair to said computer readable program code means for decrypting the encrypted data.

3. Detailed Description of Invention

Technical Field

The present invention relates in general to apparatus and method for protecting digital video/audio data and, more particularly, to an apparatus, method and computer program product for encryption/decryption of data within a computer system for communication from a CPU to an accessible internal structure, such as memory or a bus, without exposing the data in unscrambled form at the accessible structure.

Background of the Invention

Within the past decade, the advent of world-wide electronic communications systems has enhanced the way in which people can send and receive information. In particular, the capabilities of real-time video and audio systems have greatly improved in recent years. In order to provide services such as video-on-demand,

video conferencing, and digital video disc (DVD) motion pictures, an enormous amount of bandwidth is required. In fact, bandwidth is often the main inhibitor in the effectiveness of such systems.

In order to overcome the constraints imposed by existing technology, compression systems have emerged. These systems reduce the amount of video and audio data which must be transmitted by removing redundancy in the picture sequence. At the receiving end, the picture sequence is uncompressed and may be displayed in real time.

One example of an emerging video compression standard is the Moving Picture Experts Group ("MPEG") standard. Within the MPEG standard, video compression is defined both within a picture and between pictures. Video compression within a picture is accomplished by conversion of the digital image from the time domain to the frequency domain by a discrete cosine transform, quantization, variable length coding, and Huffman coding. Video compression between pictures is accomplished via a process referred to as "motion estimation", in which a motion vector plus difference data is used to describe the translation of a set of picture elements from one picture to another. The ISO MPEG2 standard specifies only the syntax of bitstream and semantics of the

decoding process. The particular choice of coding parameters and tradeoffs in performance versus complexity is left to the system developers.

Digital Versatile Disc (DVD) is an emerging technology which due to its nature, requires extensive encryption in order to protect the data, such as a motion picture, against unauthorized copying.

DVD is a specification for the content of video, audio and other compressed data to be used as playback video, audio and, for example, subtitle data by a DVD decoder. The DVD video data is specified in the Moving Picture Experts Group (MPEG) standard (ISO/IEC 13818-2). As well as being represented by this standard, the data is also encrypted using the industry's Content Scrambling System (CSS), which produces an encrypted, encoded data stream for DVD playback. The data stream can be decrypted by hardware licensed to perform CSS decryption.

Conventionally, CSS decryption occurs at a PCI card, which also conventionally includes MPEG decompression of the encrypted, encoded data signal.

The present invention is directed in one particular aspect to improving upon this conventional DVD processing of the encrypted, encoded data stream.

Disclosure of the Invention

Briefly summarized, this invention comprises in a first aspect apparatus for processing a scrambled data stream within a computer system having a central processing unit (CPU) coupled to receive the scrambled data stream. The apparatus includes a descrambling means within the central processing unit to descramble the received, scrambled data stream and thereby produce a clear data stream. Re-encryption means also within the central processing unit re-encrypts the clear data stream to produce an encrypted data stream, wherein the scrambled data stream is produced from a different encryption algorithm than the encrypted data stream. Means are provided for transferring the encrypted data stream from the central processing unit to a second structure of the computer system, the second structure being coupled to the CPU. Decryption means coupled to the second structure receives the encrypted data stream for decrypting and produces the clear data stream therefrom, wherein the clear data stream is unexposed when transferred from the central processing unit to the second structure coupled to the CPU, while the descrambling means within the central processing unit accomplishes software descrambling of the received, scrambled data stream. In another aspect, apparatus is provided for processing a data stream within a computer system

having a central processing unit coupled to receive the data stream. The apparatus includes encryption means within the CPU for encrypting identified copyright data within the data stream to produce therefrom encrypted data. Means are provided for transferring the encrypted data from the central processing unit to a structure of the computer system coupled thereto, wherein the copyright data is only transferred from the CPU as said encrypted data. Decryption means are coupled to the structure receiving the encrypted data for decrypting the encrypted data.

Various enhancements to each of the aspects summarized above are also described and claimed. In addition, corresponding methods and computer program products are presented and claimed.

To restate, in accordance with this invention clear data, whether compressed or uncompressed, is not allowed to be resident in an accessible computer system structure, such as a host memory buffer or system bus to prevent theft of the clear data. The invention is particularly applicable to MPEG encoded and CSS encrypted video data such as employed by digital video disc (DVD) technology. The decryption techniques presented herein allow for subsequent changes, for example, through the flexibility of downloading new microcode, of an

encryption/decryption algorithm pair. In addition, the particular scrambling/descrambling algorithm employed may vary. The concept is to initiate the descrambling process by host software, rescramble the data at the central processing unit using a different encryption technique, and then complete the descrambling at the receiving module, whether the receiving module comprises an additional software module executing on the central processing unit or a receiving hardware device, such as a decoder resident on a system bus coupled to the central processing unit. The rescrambling subsequent to primary software descrambling of the received encrypted data may be complete or partial. At the receiving module, the rescrambled data can be decrypted for display, output via an audio card, or undergo further processing.

Best Mode For Carrying Out The Invention

Generally stated, the present invention comprises an apparatus, method and computer program product for processing a data stream scrambled, for example, by employing content scrambling system (CSS) technology. As one aspect, the invention comprises descrambling a received CSS encrypted signal at a central processing unit without subsequently exposing a clear copy of the descrambled data in any

accessible structure outside the CPU, such as memory or a system bus. This insures that information to be protected, such as security data or copyrighted material (herein collectively referred to as "copyright data"), will not be exposed at a point where illegal copying of the original data stream is feasible (e.g., during data transfer) while still allowing software descrambling of the CSS encrypted stream. In a specific example discussed herein, the encrypted stream might also comprise an encoded stream of video/audio data compressed employing the Moving Picture Experts Group (MPEG) standard (ISO/IEC 13818-2).

In accordance with the present invention, a primary software module within a central processing unit conducts CSS descrambling and then encrypts the data stream using a selected encryption/decryption algorithm before sending any copyright data to a software module and/or hardware device outside the CPU, for example, through memory or a system bus. The external software module and/or hardware device receiving the re-encrypted data stream then decrypts the stream and processes it, e.g., for display in the case of video data or output to an audio card in the case of audio data.

Briefly summarized, the processing invoived herein includes determining at the primary software

module whether data needs to be protected during subsequent transmission from the computer system's CPU. If "yes", then the primary module communicates to the software module and/or hardware device ultimately to receive the stream of data to establish an encryption/decryption algorithm pair. This communication may involve downloading the decryption algorithm into the receiving software module and/or hardware device or signaling the decrypting software/hardware which decryption algorithm from a plurality of predefined encryption/decryption algorithm pairs is to be used. The primary module uses the selected encryption algorithm to re-encrypt the descrambled data for transfer through any accessible structure, such as memory and/or system buses, to the receiving software module and/or hardware device which is to accomplish the final decryption. The receiving module, which may also be located within the central processing unit, then decrypts the data and performs conventional processing thereon. As an alternative example, the re-encrypted data from the central processing unit may be sent through system memory and/or a system bus to a video decoder for descrambling and then decoding of the data, e.g., for display.

Fig. 1 depicts one embodiment of a computer system to employ apparatus in accordance with the present invention. A primary software module 10 and

a secondary (or receiving) processing software module 20 are each executed within the computer system's central processing unit (CPU). A processing unit hardware device 30 (such as a decoder) resides on one of the buses 26 of the computer system. Communication between primary software module 10 and software module 20 and/or processing hardware 30 requires data transfer through memory 25 and/or system bus 26, both located outside the CPU 11. Software module 10 contains a data processing module 21 and an encryption module 22. Data processing module 21 comprises any conventional processing to be done to the data stream, and in accordance with the present invention, also includes descrambling (such as CSS descrambling) of a received encrypted, original data stream. Processing module 20 contains a decryption module 23 and a processing module 24, while processing hardware device 30 includes a decryption device 27 and a data processing device 28. Original data arrives at the central processing unit 11, for example, from an external storage device or from a computer system network. This data may contain a portion which needs to be protected from illegal copying. This portion is denoted "copyright data" herein to distinguish it from the original data. If the entire original data needs to be protected, then the copyright data is equivalent to the original data. The original data is first

transferred to the input of module 10 for processing by data processing 21. Again, for example, this may include descrambling of CSS encrypted original data. The identified copyright data is then re-encrypted by encryption module 22 using a different encryption algorithm, i.e., an encryption algorithm other than CSS encryption. The original data passing through module 10 can comprise an unencrypted data stream or an encrypted data stream. In the first case, processing module 21 processes the original data and encryption module 22 performs an encryption algorithm to encrypt any copyright data. By way of example, the encryption algorithm could be of the type described in B. Schneier, Applied Cryptography, John Wiley & Sons Inc., 2nd Ed. (1996).
In the second case, processing module 21 can decrypt the original data, after which encryption module 22 would re-encrypt the copyright portion of it using a selected encryption algorithm, which again can be of the type described in Applied Cryptography. This procedure is called trans-encryption. Alternatively, processing module 21 can choose not to decrypt the original data and module 22 could then encrypt on top of the originally encrypted copyright data. This procedure is referred to as layer-encryption. Advantageously, trans-encryption allows the encryption algorithm employed within the computer system in accordance with this invention to be

different from that employed by the original data, e.g., CSS encryption. Layer-encryption allows multiple encryption algorithms to be employed, thereby enhancing security.

The encrypted copyright data can be transferred to/through system memory 25 and/or system bus 26 for ultimate receipt by secondary processing module 20 and/or processing hardware device 30. As noted above, module 20 has a decryption module 23 and a data processing module 24, while hardware device 30 contains a decryption device 27 and a data processing device 28. Decryption module 23 and/or device 27 decrypts the data encrypted by encryption module 22. The decrypted data is then processed by the data processing module 24 and/or data processing device 28, respectively.

The encryption/decryption algorithm pair employed by encryption module 22 and decryption module 23 (and/or device 27) can be a default algorithm pair predefined in the design stage of modules 10 & 20 and/or hardware device 30. Alternatively, the algorithm pair can be a downloadable algorithm.

For example, there can be multiple encryption algorithms built into encryption module 22 and multiple decryption modules built into decryption

module 23 and/or decryption device 27. Only one matched pair will be used at any given time. Before encryption, the encryption module 22 sends a signal to module 23 and/or device 27 to notice them which particular algorithm module 22 will employ. This signal can be in the form of a software parameter, or a software or a hardware interrupt. The decryption module 23 and/or decryption device 27 then employs the corresponding decryption algorithm of the selected encryption/decryption algorithm pair. Since no actual algorithm content is passed between the modules and devices, the actual encryption algorithm employed will not be known unless reverse engineering is performed within the software modules and/or the hardware devices.

Alternatively, encryption module 22 and decryption module 23 (or decryption device 27) can be predefined at the design stage to include a resident encryption/decryption routine. Before encryption, module 22 would decide on an actual encryption and decryption algorithm pair to be used. Module 22 would use the resident encryption algorithm to encrypt the actual decryption routine of the selected algorithm pair to be used by the decryption module 23 and/or decryption device 27. The encryption module 22 then transmits the encrypted version of the actual decryption algorithm to module 23 and/or device 27. Upon receipt of this information, the decryption

module 23 and/or device 27 employs the resident decryption algorithm to decrypt the downloaded decryption algorithm. Module 23 then uses the descrambled decryption algorithm as a procedure call, while device 27 could load the algorithm into a programmable circuit within device 27. After completing downloading of the actual decryption algorithm, module 22 uses the actual encryption algorithm to encrypt the data, and module 23 and/or device 27 employs the downloaded decryption routine to decrypt the data. If an update of the encryption/decryption routine is desired, then a different encryption/decryption algorithm pair is selected and encryption module 22 downloads the corresponding decryption algorithm into the decryption module 23 and/or decryption device 27. After decryption is performed, the receiving data processing module 24 and/or device 28 performs any required data processing, such as MPEG decoding of a clear, compressed video/audio data signal.

Fig. 2 depicts a flowchart of one embodiment of processing to establish encryption and decryption procedures to secure the data in accordance with the present invention using the apparatus of Fig. 1. This processing flow is started when original data enters the input of software module 10 (Fig. 1). Module 10 initially determines whether the received

data needs to be protected 50. If "no", then module 22 communicates the data directly to secondary module 20 and/or device 30 at step 60. For example, in a DVD application, module 10 can examine the Copy Generation Management System (CGMS) data. If the received data needs to be protected, then at step 51 processing communicates from module 22 to decryption module 23 and/or decryption device 27 that decryption is needed prior to use of the data.

Next, processing determines whether a decryption algorithm needs to be downloaded (step 52). If "no", meaning that a default decryption algorithm is to be used, processing proceeds directly to step 54. Otherwise, the algorithm is downloaded into decryption module 23 and/or decryption device 27 at step 53.

After establishing the decryption algorithm, encryption module 22 communicates a key to decryption module 23 and/or decryption device 27 (step 54), and uses the key and the encryption algorithm to encrypt the copyright data (step 55). The encrypted key and encrypted data can be sent as a single bitstream, or separately, to module 23 and/or device 27 by way of system memory and/or a system bus. At step 56, the decryption module 23 and/or decryption device 27 uses the chosen or the downloaded algorithm to decrypt the data. Module 22 then determines whether the

encryption key should be updated 57. If "no", the encryption and decryption processing steps 55 & 56 are repeated. If desired, the same encryption key can be used until the end of the data stream transmission. Otherwise, return is made to step 54 for communication of a new encryption key to module 23 and/or device 27.

Fig. 3 depicts one embodiment of apparatus/processing for updating encryption keys pursuant to steps 54 through 57 of Fig. 2. Within module 22 there is a key generation module 79, a key encryption module 80, a data encryption module 81 and a data multiplexer module 82. Key generation module 79 generates an original key which is encrypted by module 80 and also used by module 81 to encrypt the original data. Data multiplexer 82 combines the encrypted key and the encrypted data into one data stream, which is then transmitted through memory and/or system bus 83 to the decryption module 23 and/or decryption device 27. The decryption module 23 and decryption device 27 contains a data demultiplexer module/device 84, a key decryption module/device 85 and a data decryption module/device 86. The data demultiplexer module/device 84 decouples the received data stream into the encrypted data and the encrypted key. The key is then decrypted by key decryption module/device 85 to produce the original key. Data decryption module 86

uses the original key to decrypt the encrypted data. Fig. 4 depicts a further embodiment of processing in accordance with the present invention. In this embodiment, rescrambling of the data stream is employed after CSS decryption, along with subsequent descrambling of the re-encrypted stream prior to decompression decoding in a decoder chip. The processings described are preferably accomplished within on-chip microcode.

More particularly, a bit stream is read from a DVD disc 100 into a host processor 110 where a central processing unit conducts DVD descrambling using licensed DVD keys 112. An optional tamper resistance algorithm 114 can be employed to protect the subsequent encryption process. The clear, encoded bit stream is then rescrambled 116 using any available encrypting/decrypting algorithm, i.e., other than CSS encoding. This rescrambled data is delivered to the decoder, for example, an MPEG video decoder 128. Descrambling occurs within decoder 128 subsequent to a microcode load 124 containing the corresponding bit stream descrambling microcode. The exact portions of the stream which are scrambled and then descrambled, as well as the algorithm used, may vary from release to release of the code. The data stream may comprise an MPEG video data stream 118 wherein in one embodiment one or more fields of each

picture 120 are scrambled in accordance with bit stream rescramble 116 processing such that the data stream is at least partially re-encrypted subsequent to the DVD descrambling processing 112. A decryption key 122 as well as the microcode load 124 are sent along with the video data stream to bit stream descramble logic 126 within the video decoder 128. Those skilled in the art will note from the above discussion that in accordance with this invention, clear data (uncompressed or compressed) is never resident in an accessible computer system structure, such as a host memory buffer or system bus, thereby inhibiting theft of the clear data. The invention is particularly applicable to MPEG encoded and CSS encrypted video data such as employed by digital video disc technology. The decryption techniques presented herein allow for subsequent changes, e.g., through the flexibility of new microcode loads, of a decryption algorithm which may have been broken. In addition, the particular scrambling/descrambling algorithm employed by the rescrambling technique of the present invention may vary. The concept is to begin the descrambling process by host software, rescramble the data at the CPU using a different encryption technique, and then complete the descrambling at the receiving module, whether the receiving module comprises an additional software module or a receiving hardware device, such

as a decoder. The rescrambling subsequent to primary software descrambling of the received encrypted data may be complete or partial. For example, in one embodiment, certain MPEG data can be scrambled by the host software. The host would then transmit the appropriate descrambling microcode loads or a single microcode load with an appropriate key or keys to the receiving module or receiving hardware device. At the receive module, the microcode performs the inverse of the scrambling algorithm used by the host. The key may be static or accumulated.

Further, those skilled in the art will note that the present invention can be included in an article of manufacture (e.g., one or more computer program products) having, for instance, computer useable media. The media has embodied therein, for instance, computer readable program code means for providing and facilitating the capabilities of the present invention. The articles manufactured can be included as part of the computer system or sold separately.

The flow diagrams depicted herein are provided by way of example. There may be many variations to these diagrams or the steps or operations described herein without departing from the spirit of the invention. For instance, in certain cases the steps may be performed in differing order, or steps may be added, deleted or modified. Further, although

described principally herein with reference to a single primary module, a single receiving processing module, and a single processing hardware device, multiple modules and devices of each type may be employed as apparatus in accordance with the present invention. All these variations are considered to comprise part of the present invention as recited in the appended claims.

While the invention has been described in detail herein in accordance with certain preferred embodiments thereof, many modifications and changes therein may be effected by those skilled in the art. Accordingly, it is intended by the appended claims to cover all such modifications and changes as fall within the true spirit and scope of the invention.

4. Brief Description of Drawings

The above-described objects, advantages and features of the present invention, as well as others, will be more readily understood from the following detailed description of certain preferred embodiments of the invention, when considered in conjunction with the accompanying drawings in which:

Fig. 1 depicts one embodiment of a computer system employing encryption/decryption apparatus in accordance with the present invention;

Fig. 2 is a flowchart of one embodiment for accomplishing encryption/decryption processing in accordance with the present invention;

Fig. 3 is a block diagram of one embodiment for updating keys within the encryption and decryption modules and/or devices of an apparatus in accordance with the present invention; and

Fig. 4 is a representation of one embodiment of DVD disc data stream processing using microcode in accordance with the present invention.

【図１】

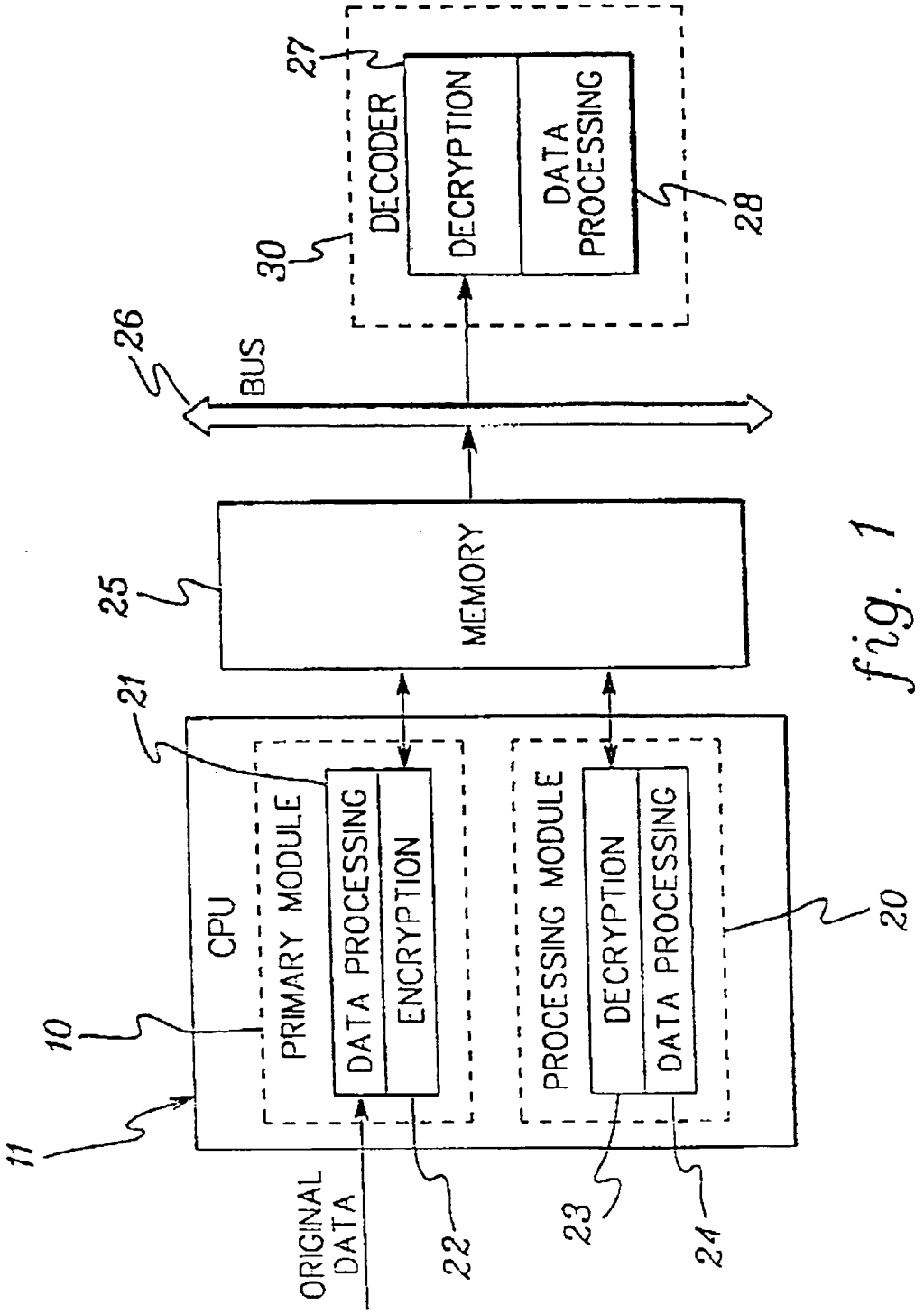

CPU
PRIMARY MODULE
DATA PROCESSING
ENCRYPTION
PROCESSING MODULE
DECRYPTION
DATA PROCESSING
MEMORY
BUS
DECODER
DECRYPTION
DATA PROCESSING
ORIGINAL DATA
10
11
20
21
22
23
24
25
26
27
28
30

fig. 1

【図２】

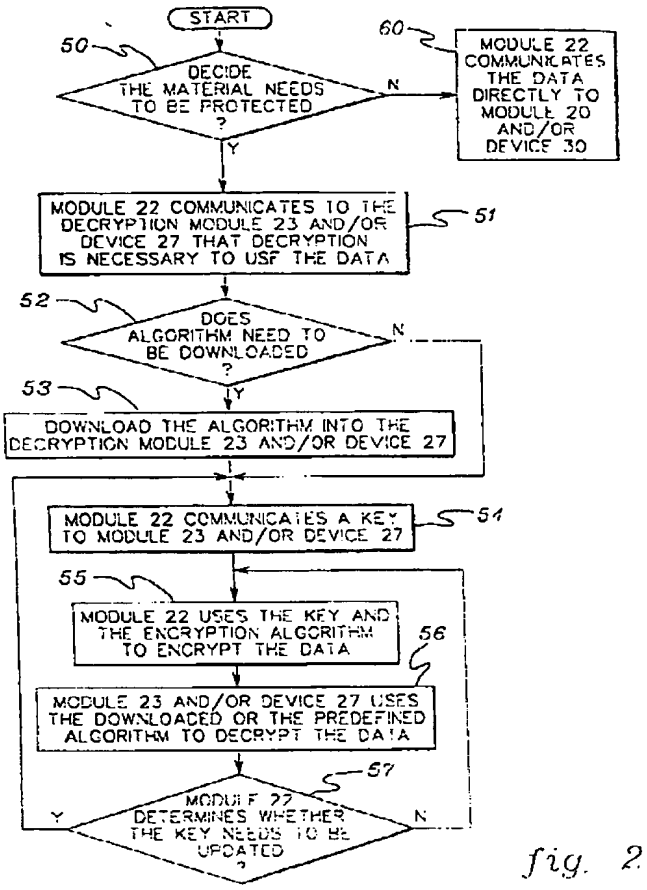

START
50
DECIDE THE MATERIAL NEEDS TO BE PROTECTED ?
N
60
MODULE 22 COMMUNICATES THE DATA DIRECTLY TO MODULE 20 AND/OR DEVICE 30
Y
MODULE 22 COMMUNICATES TO THE DECRYPTION MODULE 23 AND/OR DEVICE 27 THAT DECRYPTION IS NECESSARY TO USE THE DATA
51
52
DOES ALGORITHM NEED TO BE DOWNLOADED ?
N
Y
53
DOWNLOAD THE ALGORITHM INTO THE DECRYPTION MODULE 23 AND/OR DEVICE 27
MODULE 22 COMMUNICATES A KEY TO MODULE 23 AND/OR DEVICE 27
54
55
MODULE 22 USES THE KEY AND THE ENCRYPTION ALGORITHM TO ENCRYPT THE DATA
56
MODULE 23 AND/OR DEVICE 27 USES THE DOWNLOADED OR THE PREDEFINED ALGORITHM TO DECRYPT THE DATA
57
MODULE 22 DETERMINES WHETHER THE KEY NEEDS TO BE UPDATED ?
Y
N

fig. 2

【図３】

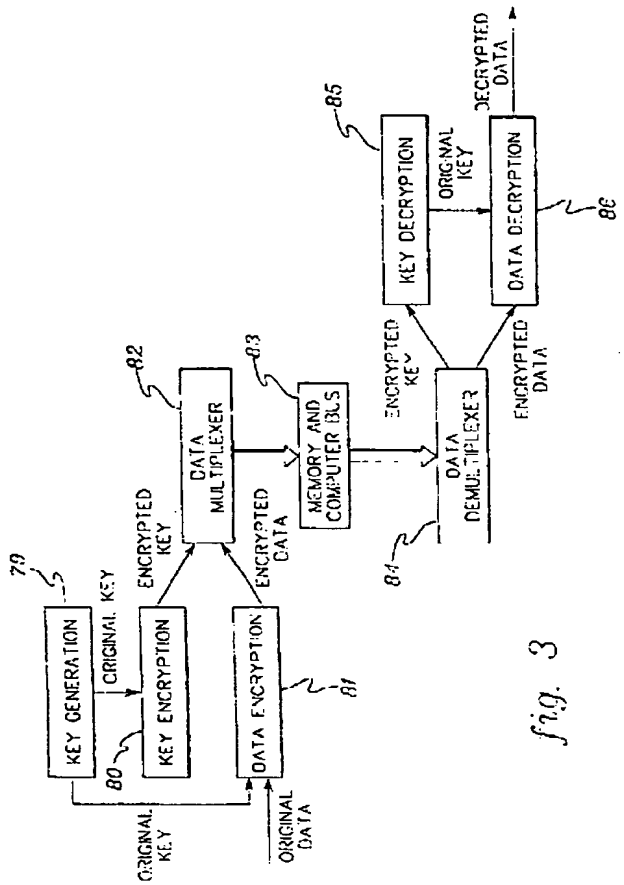

KEY GENERATION
ORIGINAL KEY
KEY ENCRYPTION
DATA ENCRYPTION
ENCRYPTED KEY
ENCRYPTED DATA
DATA MULTIPLEXER
MEMORY AND COMPUTER BUS
DATA DEMULTIPLEXER
KEY DECRYPTION
DATA DECRYPTION
DECRYPTED DATA
ORIGINAL KEY
ORIGINAL DATA
79
80
81
82
83
84
85
86

fig. 3

【図４】

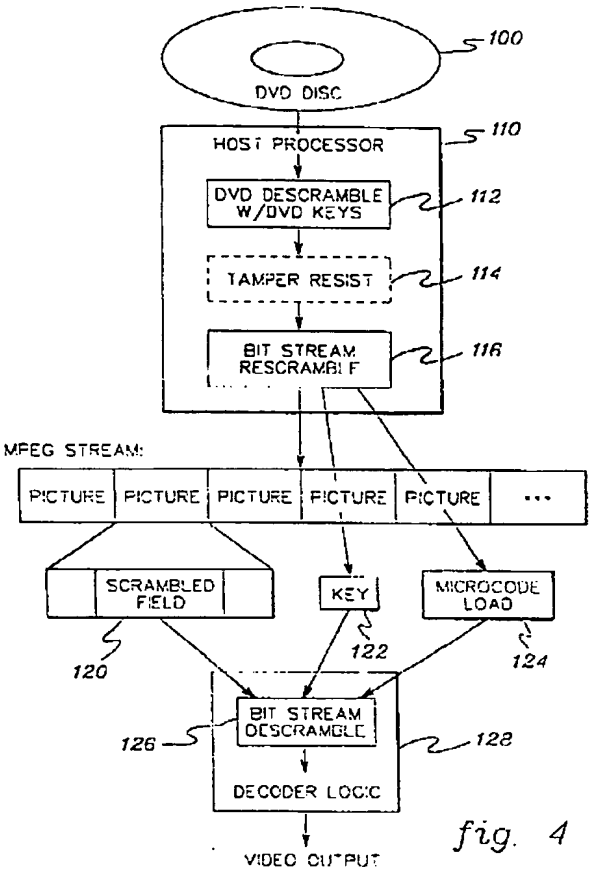

100
DVD DISC
110
HOST PROCESSOR
DVD DESCRAMBLE W/DVD KEYS
112
TAMPER RESIST
114
BIT STREAM RESCRAMBLE
116
MPEG STREAM:
PICTURE
PICTURE
PICTURE
PICTURE
PICTURE
...
SCRAMBLED FIELD
KEY
MICROCODE LOAD
120
122
124
126
BIT STREAM DESCRAMBLE
128
DECODER LOGIC
VIDEO OUTPUT

fig. 4

１．Abstract

Apparatus, method and computer program product are provided for digitally processing an encrypted data stream scrambled, for example, according to content scrambling system (CSS) technology. This digital processing insures against communication of clear data within the computer system from a central processing unit (CPU) to any accessible structure, such as memory or a system bus. Descrambling of the (CSS) scrambled data stream occurs within a module executing on the CPU, which is followed by re-encryption of the data prior to transfer from the CPU. By so processing the data, integrity of copyrighted material is maintained, while allowing for software descrambling of the CSS encrypted data stream. Various techniques for establishing the encryption/decryption algorithm pair employed are described. Decryption of the re-encrypted data can occur at a receiving software module and/or a receiving hardware device, such as a decoder.

２．Representative Drawing

ＦｉＧ１